03D004I
Project Number: BMV-C033

DATA PROTECTION ACT COMPLIANCE

An Interactive Qualifying Project

submitted to the

London Borough of Merton

and to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfilment of the requirements for the

Degree of Bachelor of Science

by

Paola Chicarelli **Michael DeNoia**

Matea Peterson **Christian Roy**

Date: February 28, 2003

Approved:

Professor Jeanine D. Plummer, Advisor

Professor Bogdan Vernescu, Advisor

Keywords: Data Protection
Training Plan
Awareness

Executive Summary

One of the most valuable resources available today is information. This is a driving force in today's economic and political spheres. Many companies buy and sell personal information. In addition, data have proven invaluable to governments in the protection and regulation of their respective sectors. However, with the increasing use and necessity of personal information, individual's rights have become a subject of great concern. The misuse of an individual's information can have a large range of adverse effects on a person. This could range from unwanted telephone calls as a result of unapproved disclosure of an individual's phone number, to denial of employment due to unauthorised release of criminal records. In an effort to minimize the abuse of this information it is important to limit the availability of personal data.

Many governments of technologically advanced states have recognized the problem of personal information accessibility. Among these are the European Community and the United States. They have reacted to this issue by passing legislation that controls the use, storage, transfer and destruction of personal data. In 1984, the UK adopted legislation to deal with information security concerns. However, as technology advanced and the use of computers became standard, new data protection issues arose. In order to maintain a satisfactory level of security, the Data Protection Act of 1998 was instated. It consists of eight principles that guarantee the rights of an individual with respect to his or her personal data.

The Data Protection Act of 1998 clearly defines the manners in which personal information is to be collected, kept, and processed. However, the knowledge of these regulations among individuals with access to personal data is limited. The Data Protection Officer in the London Borough of Merton feels that the Borough employees have inconsistent levels of data protection education and are in need of further training to comply with data protection regulations.

In order to address the problem presented, the current levels of awareness within the London Borough of Merton were assessed. As there are many diverse functions performed by the Borough, we studied each of five departments individually, as well as the Borough in its entirety. This assessment process had two phases. The first involved interviewing members of management, and the second involved surveying employees working in the Civic Centre.

In the first phase, we selected eight interviewees on the basis of their positions. There was at least one interview conducted per department, and each interviewee was a member of middle or upper management. They were questioned regarding their perceptions of the Data Protection Act's use and effectiveness within their departments. Each interviewee was first asked about the relevance of data protection to his or her department's work. They were then asked questions regarding practical use of each of the eight principles within the department. In addition, each was asked about the training of their subordinates to discover what level of data protection training was typical. Lastly, we examined the methods of education and communication that were used as well as their effectiveness.

We constructed surveys in the second phase based on the information obtained from the interviews. The surveys were divided into three sections. The first section asked for information that helped classify survey results. The second section contained generalised as well as department-specific questions and was designed to evaluate knowledge of the Data Protection Act. Other questions were included that covered all eight of the principles in order that no area of exploration would be neglected. The third section was focused on the respondent's opinions and perceptions of the Data Protection Act's importance and effectiveness. The survey was conducted online. Links to the survey were distributed through a global e-mail. In order to encourage employees to take the survey, we entered respondents into a raffle.

We analysed the data gathered from our surveys and interviews. We found that the majority of managers interviewed stated that their employees had basic knowledge of the Data Protection Act of 1998, but not of the specific regulations and application. Likewise, over three quarters of the survey respondents described themselves as "generally aware, but not of details" of the act. Of the specific regulations, there were three areas of data protection that were the most problematic. First, there was the issue of interdepartmental security. Employees were largely unaware of which data may or may not be transferred between departments. The second recurring issue was the knowledge of data subject request regulations. Only 7% of Civic Centre employees were aware of the time allowed for answering such requests. However, a large majority was aware of the legal consequences for not complying with data subject requests. The last common matter was the amount of outdated information. Several managers in different departments stated that there was a large quantity of data that was not up-to-date. They said that departments lacked the policy and staff to keep information current.

In addition to the data gathered about Data Protection Act compliance, our group researched education and training methods at the London Borough of Merton. Managers we interviewed reported that the most effective means of communication in departments were seminars and team meetings. Furthermore, they suggested that the data presented in these manners be reinforced with written material. Survey results also showed that employees preferred seminars and team meetings. Among educational tools that can be used for reinforcement, pamphlets were best received. However, manuals were preferred in two departments.

From the information analysed, our team developed a set of recommendations for departmental educational plans. We recommended that there be a common section in each educational plan. This section would include a basic overview of the Data Protection Act. It would also address the three

main concerns of interdepartmental security, data subject requests, and outdated information. Following this, each departmental training plan would consist of matters that were of concern to that particular department. Each training plan would be presented in the manner shown to be the best received in that department. Following the presentation of data protection information, departments would receive a manual or set of pamphlets to serve as a reminder and reference.

Abstract

We conducted an analysis of Data Protection Act awareness for the London Borough of Merton. This act ensures proper storage and use of citizens' private information. We interviewed managers and surveyed employees about awareness of the Data Protection Act, as well as methods for educating personnel. Results showed that most employees were generally aware of the act, but not of specific regulations. From the gathered data we formulated recommendations for general and departmental training plans.

Table of Contents

List of Figures

List of Tables

Chapter 1 – Introduction

One of the most valuable resources available today is information. This resource is the driving force behind a large portion of the economy. Many companies buy and sell information. There are also those who offer services dependent upon data collection. For example, Fidelity Investments International (who requires large amounts of personal financial and stock information) and Patrick Marketing Group (a company that buys people's information for telemarketing purposes) are two corporations whose existence is dependent upon information. In addition to economic value, data have great worth to governments. Information is paramount in the protection and regulation of a nation. However, this information is not solely statistical data concerning inanimate objects. Many times the data held by corporations or governments are personal.

As larger and larger amounts of information about individual citizens have been collected, society has become increasingly concerned with data privacy (Ayoade and Kosuge, 2002). Consequently, it is necessary to examine the possible consequences of information availability. The issue of personal data accessibility has many practical implications. The indiscriminate availability of one's information may have a wide spectrum of adverse effects. For instance, easy access to such information as addresses, phone numbers and financial records are a source of safety concerns (Wright, 1998). If one's medical or criminal records are easily obtained, it can raise issues of discrimination (Donaldson, 2000). The far-reaching effects of personal data privacy affect nearly every area of one's life. A person's records need to be guarded in order to minimize potential damage done to the individual.

Governments and law makers have long realised the problem of data protection. Legislation has been passed in most modern countries that addresses information security. The United Kingdom (UK) is perhaps one of the most advanced in this regard. As such, it passed a new Data Protection Act in

1998, in order to update its predecessor passed in 1984. This law was brought into effect in March 2000, and was analogous to the legislation passed in the European Community in 1995. Under this new law, personal information security is dictated by numerous regulations. The 1998 legislation is concerned with computerised personal data as well as personal data held in structured manual files. It regulates anything pertaining to personal data processing, including collection, utilization, exposé, destruction and storage of data. Additionally, there are criminal charges associated with breaking these directives.

The Data Protection Act of 1998 clearly defines the manners in which personal information is to be collected, kept, and processed. However, the knowledge of these regulations among individuals with access to personal data is limited (Guild, 2003). In our case, the workers of the London Borough of Merton have inconsistent levels of data protection education. The Data Protection Officer feels that these employees are in need of further training in order to comply with personal data regulations. Therefore, our project goal was to measure the current levels of awareness and create a plan to heighten and improve the employees' knowledge of regulations.

In order to measure employees' awareness, we interviewed members of the management and surveyed each department. Also, we utilized interviews to determine the obstacles that hinder compliance. Once these factors were established, we created recommendations for a communications plan. Once developed, this plan's goal will be to raise awareness of regulations as well as the importance of data protection. We expect that once employees are aware of the rules they are to follow and their importance, compliance with directives will increase.

In order to understand Data Protection Act compliance in the London Borough of Merton, certain background information is necessary. The next chapter presents information on various data protection legislation as well as training methods. Following this, we discuss the methods we implemented to confront the Borough's issue of data protection compliance. We also give the information gathered with these methods. Finally, we present the conclusions that we drew from this data, as well as further research that is needed.

Chapter 2 - Background

To assess the awareness of the Data Protection Act, an enhanced understanding is necessary in three areas: 1) data protection, 2) training and compliance, and 3) specific elements within the Data Protection Act of 1998. Once these areas were analyzed in depth, we had a better understanding of the Data Protection Act of 1998.

2.1 Data Protection

Data protection is characterized by the need to enforce certain legal requirements with regard to the way in which personal information is dealt with in today's technological society. The need for data protection came into being as a result of the rapid evolution of computers in the 1970's. Consequently, the threat to personal privacy quickly arose, as did the rapid abuse of personal data. Personal data was easily exposed to other individuals (Branscomb, 1995).

Data protection refers to efforts of individuals to protect this personal information and control its usage. It is of concern to individuals that their private information will be used or applied in a safe manner and that violation of their basic "human right of privacy" will be strictly prevented (Carey, 2000, p. 9). The use of data protection ensures that personal data about any individual is processed in accordance with legal requirements in order to protect the rights of that individual. Companies, organisations, and individuals need to be aware that they may be dealing with information detailing a person's private life. Such details should be handled with care and respect.

2.1.1 Importance of Data Protection

It is very easy to access information from individuals' personal lives and daily activities. For example, people are often willing to supply personal information with the promise that they will be rewarded in

some way for doing so. They may either be rewarded by receiving airline miles, lottery entries, or product samples. Similarly, a variety of information may be acquired about individuals as they go about their daily routines whether browsing the internet, withdrawing money or subscribing to magazines. The need for data protection is vital, as it is easy to acquire personal information such as addresses, emails, and dates of birth. Due to the ease with which this can be done, the consequences of acquiring personal data should not be overlooked. Security of data ensures that the transmittance of unauthorized or inaccurate data will not lead to refusal of credit, housing, or employment (Kennedy, 1995).

The twenty first century has been the first in which personal information has been given so freely to the commercial sector (Branscomb, 1995). People might think of the ease of gathering information as a positive evolution and intelligent use of modern technology. However, there are opportunities for severe misuse in both the private and public sectors due to the great quantity of information that is available.

An example of how personal information can be improperly used is illustrated by the Beverly Dennis case. Ms. Dennis was a victim of inadequate data protection. She was a grandmother from Ohio who had completed a questionnaire for the Metromail Corporation, a direct marketing firm, in order to receive free product samples. She gave out personal information such as her income level, date of birth, divorce status, and interest in physical fitness. Ms. Dennis not only received free product samples, but a "sexually graphic and threatening" letter from a convicted rapist in a Texas penitentiary (Wilson, 1997, p. 3). Due to her willingness to answer a questionnaire, her personal information was taken and abused. As a result of this, a convicted prisoner was able to obtain her personal information and hassle her. This happened because the Metromail Corporation subcontractor used poor judgment

and made use of the prisoners to enter questionnaire data into a database. This unfortunate situation occurred because it is very easy to get hold of information regarding people's personal interests, consumer habits, and private lives (Wilson, 1997).

People are concerned about the unauthorized use of facts over which there is no control and for which there seems to be no practical legal protection. The government tries to recognise individuals' rights in an attempt to keep back personal information and prevent intrusions upon private information environments. Laws for data protection are required to keep individual's data safe. Such laws protect personal information (names, addresses, birth and death certificates, and annual income records). The majority of information held on individuals is private, thus the laws must specify who may be granted access, while also maintaining the privacy of the individual.

2.1.2 Privacy

People strongly believe they have legitimate rights to their privacy. Privacy laws exist primarily in the interest of protecting individuals' private space into which outsiders should not be permitted to penetrate (Branscomb, 1995). One of the primary foundations of data protection is the Right To Privacy. The Right to Privacy is provided for in the European Convention on Human Rights and has been defined as "the right to be left alone" (Kennedy and Alderman, 1995, p. XIV). The main objective of data protection law is to ensure that the fundamental right to privacy is not abused in the rapid growth of modern technology.

An example of privacy abuse is illustrated in the following case. The mother of an eleven-year old child attending a London primary school sent a complaint claiming that her child, while in school, had been electronically fingerprinted for a new library system. The problem was that it had been done without the consent of the parents or understanding of the children. Later it was discovered that the

system employed on her child was sold to about 1,000 schools. This technique was used to replace library cards and to increase efficiency of library. This example addresses the deep concerns about the issue of privacy. Therefore, the Data Protection Act (see Section 2.4) explains how privacy is being protected in today's modern society.

The concern with privacy has become more apparent as a result of the rapid spread of information of individuals' daily lives. Privacy covers such a wide spectrum of individuals' lives that it is hard to formulate an exact classification for it. There has been extensive debate in Washington D.C. regarding the specifics of that issue, as there has been in many countries of the world. Almost "1,000 of 7,945 bills introduced in the 104th Congress include the privacy issue" (Cate, 1997, p. 1). However, these bills have resulted in few new directives and regulations. Privacy has been the topic of many scholarly books, journals, conferences, articles, Acts, reports, and discussion groups, and still much debate exists surrounding the issue of privacy. This leads to little consensus of what privacy really represents and who has the right to it (Bushkin , 1976).

2.1.3 Ownership of Information

Debate over the ownership of information in today's society is a very controversial issue. Today many countries have become information dependent. The public is worried about how laws will provide them with protection to prevent improper access of their information (i.e. patents, copyrights, and trade secrets). The ownership of personal data is a large issue. For example, if an organisation places a telephone call to an individual, does that organisation have ownership of the information obtained? What rights does the data subject retain? The answers to such questions are contained within data protection legislation. The dilemma comes with keeping data users aware of their responsibilities and ensuring that they are properly trained to do so.

2.2 Data Protection Awareness, Compliance and Training Methods

It is necessary for corporations to train their employees to maintain regulatory compliance and conformity with data protection principles (Carey, 1998) his issue of how best to train employees to comply with regulations is one of extensive study. The design of a training program is a lengthy process. First, managers must try to determine why their employees are not complying with regulations. There are many possible reasons for non-compliance. For example, it may be an issue of attitude or a lack of knowledge. Secondly, managers must choose the best method for remedying the problem (Loughary, 1979). In order to do this, managers must look at available methods and determine which system is best for the current situation. In this section we first discuss manners of measuring awareness and compliance. Then we examine reasons for non-compliance and the best means for resolving this problem.

2.2.1 Measuring Awareness and Compliance

When authorities aim to assess the compliance of individuals with any set of regulations, they encounter the issue of how best to accurately measure this. This performance appraisal is a constant source of problems, however it must be done (Furnham, 1998). Several options are available. First, they may observe the actions that necessitate compliance. Alternately, they may ask either the persons to be evaluated, or the persons' superiors, about the extent of the individual's observance of guidelines. Lastly, awareness can be assessed with the assumption that awareness yields compliance.

The first mode of assessment, direct observation of compliance, is time-intensive. It may take an extended period of surveillance for the evaluator to determine the level of compliance. Behaviour "can take months to measure and for most involves considerable effort" (Furnham, 1998, p. 207). Some case studies of individual and group behaviour even last years. For example, a study evaluating the enhancement of compliance with California safety regulations took two years (Stokols and Clitheroe

and Wells, 2001). This study assessed forty-eight small and medium sized companies. The researchers implemented a program and then evaluated compliance twelve months afterward. A reasonably long period of time is necessary in order to produce a study that evaluates a representative sample of the analysed population. In addition, it is important that assessments are repeated regularly in order to ensure their validity (Furnham, 1998). Both of these factors contribute to the extensive time requirements of direct compliance observation.

The second method is the evaluation of compliance through questioning the employee or his or her manager. This has severe limitations. When interviewing an individual about conformity with regulations, there exists the strong probability that the individual will answer in his or her own favour. Secondly, there is a great variability in truthfulness between individuals. Many personality features affect a person's response when asked about personal guilt (Gozna, Vrij and Bull, 2001). This inconsistency makes it difficult to determine the accuracy of the results. If managers are questioned about their workers' compliance, they have the disadvantage of limited knowledge. Managers are incapable of informing themselves completely about the actions of each of their subordinates. In addition, there is the issue of the objectivity of a manager's appraisal. For example, a manager may be influenced by preconceived notions of performance (Gomez-Mejía, Balkin and Cardy, 2001).

The method of indirect measure is the most objective system of evaluation. Indirect measure evaluates the subject's awareness of directives. It is therefore possible for the assessor to obtain information without the interference of personal opinion (Gomez-Mejía et. al., 2001). With this manner of assessment however, one cannot be assured that the measured awareness will yield compliance. On the other hand, one can be guaranteed that an individual cannot fulfil regulations without such knowledge.

2.2.2 Compliance in Organisations

To determine the reasons employees do not comply with regulations, it is helpful to first examine the motivations they have for following such rules. Some reasons for compliance are strong regulation enforcement and attitudes of management and employees toward the regulations. However, there are other motives individuals have for following rules.

It seems intuitive that employees within an organisation would comply with regulations because the organisation is frequently monitored in an effective means, and because the law is adequately enforced (Dasgupta, Hettigae and Wheeler, 2000). However, recent studies show that many associations fulfil decrees without being monitored. The apparent lack of incentive presents the question of why this is done. In some cases, it appears that "publicly-spirited" managers were responsible (Dasgupta et al., 2000, p. 41). In other cases, economic consequences with non-compliance for the organisation may be the driving motivation. Other researchers conclude that although one many believe that workers must be driven to comply by fear of penalty, they will actually drive themselves if they believe compliance is important (Simpson, 1989).

Another factor that can affect compliance is the attitudes of base-level employees and managers. Many studies have shown that attitudes affect behaviour. In these analyses, "attitudes are considered to be 'casual' factors influencing behavioural intentions as well as behaviour" (Torbjorn and Hale, 1995, p.1). In Torbjorn's study of managers' attitudes and their effects on safety compliance, it was found that the attitudes significantly influenced observance of regulations. However, in this specific study, the respondents were 96% male and worked in a company that deals mostly in petroleum, aluminium and agricultural products. It is not a blanket application to other situations. As the author says, "attitudes are specific to objectives and situations, and therefore one should be careful not to

generalize…" (Torbjorn and Hale, 1995, p. 16). However, attitudes in many situations, including this one, can have a great effect on the compliance of managers and resultantly on their subordinates.

2.2.3 Training

A widely-accepted method to enhance compliance is training (Loughary, 1979). Although there are many forms of training, there are some universal concepts essential to all effective educational programs. First, all training must utilize good communication techniques. Secondly, employees' sources of motivation and resistance must be known. This is an essential supplement to training. William Simpson states that, "Assuming that employees are given the opportunity for good performance and have the necessary skills, then effectiveness depends on motivation" (Simpson, 1989, p. 2). Therefore, in order for a training plan to be effective, employees must be motivated to use the knowledge acquired from it.

2.2.3.1 Effective Communication

When developing a training plan, one of the most important aspects is communication. Regardless of how well thought out the rest of the plan is, if information is not communicated effectively, the training will not yield results. There are several key aspects of communication that are important for good training plans (Bergin, 1990). These include clarity, completeness, and concision. Information passed down to employees must be clear. Information must be simple as this provides for higher levels of comprehension (Adair, 1973). Next, communication should be complete and must provide all of the information that is expected to be known (Bergin, 1990). Lastly, information must also be concise. In addition to remembering the value of employees' time, it is important to realise that individuals' attention spans do not usually allow for lengthy messages. Bergin notes that the timing is also important to any message's reception. He says, "Even where there is no absolutely good time the

really bad time can usually be avoided (Bergin, 1990, p. 6).” Beyond the communication basics, there are many different modes of communication that can be used in training.

2.2.3.2 Motivating Change

The successful training program must effect change. However, this presents a problem since most individuals are resistant to change due to “ingrained behavioural habits” (Furnham, 1998, p. 45). Therefore, when developing a training program, managers must also consider how to motivate their subordinates to apply knowledge learned in the training. First, one must examine why employees are resistant to change. Most resistance is motivated by fear (Simpson, 1989). These fears include fear of job loss, inability to cope with change, loss of familiarity, and loss of skills.

Once it is clear why individuals resist change, an individual should determine a way to deal with this resistance. Simpson says that “communication and consultation are particularly important in times of change” (Simpson, 1989, p. 18). Individuals must be informed of changes before they are implemented. Then they must feel that they have a right to supply feedback about these adjustments.

2.2.4 Effectiveness of Different Training Methods

There are many methods currently available to companies for educating and training their employees. Different systems of training offer distinct attributes that are valuable in different situations (Gomez-Mejía and Balkin and Cardy, 2001, p. 262). In addition, different people prefer different teaching styles (Furnham, 1998). Therefore, there is not any one method of training that is always superior to another. The effectiveness of training processes depends on the circumstances in which they will be implemented, as well as the individuals to whom they will be applied. Here we examine several training methods including their strengths, weaknesses, and the conditions under which they are most useful.

2.2.4.1 Classroom Style Instruction

The most widely-implemented method of training is instruction. This style accounts for the vast majority of all adult training (Craig, 1976). In this method, individuals are taught by an instructor who is an expert in the area of education. This classroom style of raising awareness has advantages such as flexibility and low cost. It allows the instructor to use a wide variety of approaches to teaching, from visual aids to teaching in small groups.

Classroom-style teaching also has some drawbacks. Classroom training has the distinction of being "the most ill-used of all the possible techniques" (Craig, 1976, ch. 33 p. 2). Therefore, it is important that certain qualifications are met before using a classroom approach to training. Primarily, the trainer as well as the trainees should have a good understanding of the deficiency to be repaired (Craig, 1976). Because the classroom instruction method is so widely misused, it can be useful to look into other training possibilities.

2.2.4.2 Learning-by-doing Strategy

A learning-by-doing strategy is another method of improving awareness of regulations. Here, an individual learns by actually doing tasks instead of simply learning generic philosophies. This method employs interactive measures that heighten interest, but also tends to raise the cost (Loughary, 1979). This method was implemented in a study focused on the management of 100 different companies (Hakkinen, 1995). In this case, the persons involved took part in short training sessions described as a "real decision-making situation." It was found that this method was a useful alternative to the usual seminar (Hakkinen, 1995). Furthermore, the researchers state that the training and education of decision-makers is essential for creating "commitment to action" (Hakkinen, 1995, p. 300). However, Hakkinen states that this method of training is restricted and can only be applied to those who are in management positions, specifically those who make decisions.

2.2.4.3 Handbooks

Handbooks provide a third way for improving employee awareness. An example of this method in use is provided by a case study done in Norway (Karina, 1998). In this case, knowledge transfer was attempted by passing on instruction manuals, rather than directly training employees. Although this method is useful in that it provides the trainee with a permanent, accessible source of information, it can also produce a sense of resentment. Karina notes that this resulted in "a sense of duty" among those receiving the handbooks, as the employees felt that they had to read the handbooks but did not want to. Furthermore this educational method produced a feeling that the handbooks had "no practical importance," as they were uninteresting and difficult to understand (Karina, 1995, p. 226). The researcher concludes that necessary aspects to successful handbook use were: availability, content simplicity, minimal document volume, and minimal bureaucracy.

2.2.5 Summary

Employees have many different motives for compliance and non-compliance with regulations. It is important that managers examine the particular cause of non-compliance in their subordinates before choosing a method with which to remedy that non-compliance. Once informed about employees' motivations, managers can examine the various methods of training and determine which of them is most suitable for the type of information to be communicated, the people to whom it is to be given and the available budget.

2.3 Legislation

In order to protect the data of individuals, specific regulations have been established to define the extent to which the individuals are protected. Regulations typically specify, for example, what types of data are permitted, circumstances in which those requirements are exempt, and methods of enforcement. The regulations can be small or large scale, covering an area such as the European

Union (multiple countries) or just a city or town. In any case, law is developed to dictate all aspects of data protection.

2.3.1 E.U. Legislation and Privacy Regulations

The concept of privacy has only been considered in government legislation within the last 35 years, in the United Kingdom or elsewhere. The first site of privacy legislation was within the European Union (EU). In 1970, the first regulations with regard to privacy were enacted in the German state, Hesse. Sweden was the first country to implement a national protective statue, employing doctrine in 1973 (Cate, 1997). The first legislation covering the entire European Union was not implemented until 1980.

Privacy legislation in the European Union typically includes four main features (Cate, 1997, p. 34). First, the legislation applies to both public and private sectors. Records incorporated in the public sector include medical and tax records, for example. Records incorporated in the private sector include information such as video titles rented or telephone calls. The second feature is the application of legislation to a wide range of activities, such as data collection, usage, and storage. Third, EU privacy legislation classically lists restrictions and requirements. It specifies regulations regarding what individuals cannot do and what they must do in order to comply with regulations. Fourth, the legislation applies regardless of the type or subject of data. Most forms of data are covered. These principles were the basis of privacy regulations set forth by the European Union, beginning with the first doctrine enacted in 1980.

In 1980, the Committee of Ministers of the Organisation for Economic Cooperation and Development (OECD) issued *The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

This doctrine outlined the basic principles for data protection and the flow of data between countries. It further contained specific laws confirming the four primary principles, though it was not considered a binding force (Boehmer and Palmer, 1993). Though specific guidelines were defined, the member countries were not required to follow them.

In 1981, the Council of Europe drafted a convention *For the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Cate, 1997, p. 34). This convention was designed to supplement the guidelines drafted the previous year, though it did not take effect until 1985. The convention specified five key points:

1. Data must be obtained and processed fairly.
2. Data must be used and stored only for legal purposes.
3. Data must be adequate, relevant, and not excessive in relation to the purpose of its use.
4. Data must be accurate and up to date.
5. Data must not be stored longer than necessary.
   (Cate, 1997, p. 34)

The convention additionally gave individuals the right to enquire about the existence of data files concerning themselves, obtain a copy of the data, and have false or improperly processed data files corrected or erased (Cate, 1997). In order to enforce these rights, European Union (EU) member countries were required to enact laws confirming the convention.

In July of 1990, the commission of the European Community (EC), later known as the EU, published a draft of the *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. The directive was drafted to better articulate the principles within previous doctrines and to attempt to create a more solid political union, as would later be contained in the 1992 Treaty on European Union (Cate, 1997). In 1992, the European Parliament amended the 1990 directive, overwhelmingly approving the doctrine. The only major

change was the elimination of a distinction between the public and private sectors (Cate, 1997). In October of 1992, the European Community issued the amended proposal.

In 1995, another doctrine was established by the European Community. In February of 1995, the Council of Ministers adopted a *Common Position with a View to Adopting Directive 94/ 46 /EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal data and on the Free Movement of Such Data* (Cate, 1997, p. 36). This was formally approved in October 1995 and was to take effect in February of 1998 (Jay and Hamilton, 1999). The directive placed further emphasis on the need for EU member states to enact laws regarding the "processing of personal data" (Cate, 1997, p. 36). The doctrine defines "processing" as "any operation or set of operations [including but not limited to] collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction (EU Directive, 1994, art. 2a). It then defines "personal data" as "any information relating to an identified or identifiable natural person" (EU Directive, 1994, art. 2b). The information noted not only includes text, but also photographs, audio/visual images (i.e. videotape), and sound recordings. In addition, this directive is not limited to "living" natural persons, but also includes the deceased. The two main contexts when the doctrine does not apply are to activities outside the scope of the European Community law (such as for purposes of national security) and in the event that the processing of personal data is performed by "a natural person in the course of purely private and personal activity" (EU Directive, 1994, art. 3 sec. 2). Some specific exemptions are as well contained within the document.

Presently, the 1994 doctrine is the primary legislation in the European Union governing the protection of data. As was emphasised within the doctrine, the individual members of the European Union were required to develop national policy acknowledging the 1994 doctrine. Members were also responsible for articulating their own regulations enacted to further support the doctrine. The United States has implemented similar legislation in order to control the use of personal data. Though based on similar principles, the interpretation of the United States legislation is considerably different.

2.3.2 U.S. Legislation and Privacy Regulations

In the United States, legislation differs depending upon the sector that it governs. Consequently, the regulations on data protection are different depending upon which sector they are being applied to. Separate legislation has thus been developed for the public and private sectors. Legislation pertaining to the public sector, as with early European legislation, applies to information which is public knowledge and on which the government holds records. This includes areas such as resident addresses, census information, and tax records. This information is typically housed in a town or city hall, and is available for limited public viewing. Information included in the private sector is restricted to a particular company and the individual to whom the information pertains. This may include records of phone calls, video rentals, or billing information. This information is not available to the general public. Of these two sectors, the public sector is more strictly regulated.

2.3.2.1 U.S. Legislation in the Public Sector

Two primary pieces of legislation are in place in the United States to govern data protection in the public sector. The first of these is the Freedom of Information Act (FOIA), enacted in 1966 (Henderson, 1999, p. 47). This act states that any individual is permitted to access records contained by any federal agency. Key in regulating those records are nine exemptions, two of which pertain specifically to data protection. Exemption 6 prohibits the disclosure of personnel information, medical

profiles, and related files, which might "constitute a clearly unwarranted invasion of privacy" (Cate, 1997, p. 77). This exemption forbids release of files containing personal information, which could be harmful to the individual. Exemption 7 prohibits the disclosure of "records or information compiled for law enforcement purposes [which] could reasonably be expected to constitute an unwarranted invasion of privacy" (Cate, 1997, p. 77). This exemption prevents release of information such as an individual's criminal record, which could, for example, be detrimental to the individual's integrity when searching for employment. The overall goal of the doctrine and exemptions is to keep the individual aware of the use of his or her personal information and to prevent its abuse. The FOIA was amended in 1974 and 1986 to ensure the success of its goals in a rapidly changing world (Henderson, 1999, p. 47).

The second piece of United States legislation that governs data protection is the Privacy Act of 1974. In this Act, there are five main principles that are advocated (ConsumerPrivacyGuide.org, 2001/2002). First, there should be no record whose existence is denied or private. Second, an individual must be able to determine what information is held on him or her and how it is being used. Third, an individual must be able to prevent information collected for one purpose from being used for another without first obtaining consent. Fourth, the individual must be able to correct inaccurate information stored on him or her. Fifth, any organisation creating, using, storing, or distributing information on an individual must assure that the data is not misused. There are twelve exemptions included in this doctrine that permit disclosure of information to government agencies. The Privacy Act of 1974 was amended in 1983, mainly to allow the government to give credit agencies personal information on people who owe the government money. The amendment also required the government to keep track of any records it disclosed (Henderson, 1999).

Other protections have been enacted since 1974, primarily as amendments to the 1974 Act to apply it to modern conditions. For example, the Computer Matching and Privacy Protection Acts amended the 1974 Act in order to establish specific guidelines for organisations to follow during matching of electronic records (Cate, 1997). The majority of amendments and further doctrines, however, are agency- or topic-specific. For example, via amendments, the Health and Human Services Department has been prohibited from distributing individuals' social security numbers and the Internal Revenue Service has been prohibited from disclosing information on individuals' income tax returns (Cate, 1997).

Other regulations have been enacted as the result of isolated incidents, in order to prevent any such occurrences in the future. An example is the Driver's Privacy Protection Act of 1994. It was enacted in combination with other legislation in response to the 1989 murder of actress Rebecca Schaeffer. Schaeffer was killed by an obsessed fan who obtained her address and other personal information from the Department of Motor Vehicles (DMV) records. The Act now prohibits the DMV and its employees from releasing personal information contained in a driver's record (Cate, 1997). Many states have also adopted legislation that reflects current federal regulations. There are, however, exemptions for government agencies, allowing them access to information when needed.

Overall, the government control of data protection is limited. It often applies to limited areas of information and to specific organisations. While the release of information is also frequently the target of regulations, the collection and use of the information is not tightly regulated. Furthermore, enforcement is impractical and therefore nearly nonexistent. Enforcement is costly, time consuming, and ineffective as regulations are not specific and provide numerous loopholes (Cate, 1997).

2.3.2.2 U.S. Legislation in the Private Sector

Regulations in the private sector are considerably different than those in the public sector, primarily due to the nature of the information being protected. Rather than the large, all-encompassing regulations of the public sector, the legislation provided covering the private sector consists of a multitude of smaller regulations targeting specific types of information. The first of such regulations is the Fair Credit Reporting Act established in 1970. This Act specified the rights of individuals and responsibilities of agencies when reporting consumer credit information (Reidenberg, 1992). This act was amended in 1996. The resultant Consumer Credit Reporting Reform Act closed some of the many loopholes by narrowing the scope of "legitimate business needs" for which credit reports could be disseminated (Cate, 1997, p. 81). Another such piece of legislation is the Electronic Funds Transfer Act of 1978. This Act established guidelines for "the relationship between consumers and financial institutions" with regard to the electronic transfer of funds (Reidenberg, 1992, p. 214). Included within the Act are transactions involving automated teller machines (ATMs), point-of-sale terminals, automated clearinghouses, telephone bill-payment systems, and home banking programs (Henderson, 1999).

Numerous directives were developed in the area of telecommunications. The Electronic Communications Privacy Act of 1986 prohibits the interception and disclosure of information in transit via electronic communication. This includes telephone, e-mail, and other modes of communication. There are many exemptions to this Act, however. For example, it does not apply if one party involved in the communications consents to disclose the information. It additionally does not apply to switchboard operators or telecommunications company employees. It further does not cover information transmitted via means that are accessible to the public (i.e. marine/aeronautical communications). Moreover, it does not limit the transmission of information obtained through an

electronic transaction (Cate, 1997, p. 84). This Act was later amended, resulting in the Telecommunications Act of 1996, in order to protect "transactional" information.

The Cable Communications Policy Act of 1984 was similarly enacted to restrict collection, storage, and disclosure of personal information through a cable subscription. The Act requires providers to inform customers of the nature of collected information, frequency of collection, and the duration of storage, and must further make available that information for review by the individual (Cate, 1997). Unlike the majority of United States legislation, this Act provides penalties for violations. Characteristic of all regulations, however, it does provide exemptions.

Numerous other pieces of legislation are in place, the majority of which dictate the same conventions. Henderson (1999) noted that they typically contain regulations on gathering, holding, and releasing data. He further stated that regulations on correcting false data have been overlooked and that the United States lacks policy on enforcing regulations. He added that by neglecting enforcement, the United States effectively undermines its attempts to protect data. Most government agencies and commercial organisations are their own judges on their level of compliance (Henderson, 1999). Lacking enforcement, many organisations have no reason to follow regulations.

Examining United States data protection legislation provides a basis for comparison when looking at United Kingdom data protection legislation. Having knowledge of United States policy allows a more effective evaluation of the strengths and weaknesses of policy in the United Kingdom.

2.3.3 U.K. Legislation and Privacy Regulations

In the United Kingdom, the issue of data protection was a rising concern throughout the latter half of the twentieth century. The issue was addressed formally for the first time in 1972, in light of the

substantial increase in the use of computers (Jay and Hamilton, 1999). At that time, the British Younger Committee on Privacy recommended ten principles in order to control the use of computers in data processing:

1. Information should be regarded as held for a specific purpose and should not be used, without appropriate authorisation, for other purposes.
2. Access to information should be confirmed to those authorised to have it for the purpose for which it was supplied.
3. The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.
4. In computerised systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.
5. There should be arrangements whereby a subject can be told about the information held concerning him.
6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuser or misuse of information.
7. A monitoring system should be provided to facilitate the detection of any violation of the security system.
8. In the design of information systems, periods should be specified beyond which the information should not be held.
9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.
10. Care should be taken in coding value judgements.
    (Carey and Russell, 2000, p. 1)

There was no legislation requiring these principles to be met by any means. The principles would be used, however, in formulating later legislation regulating data protection. The first attempt to pass data protection legislation in the UK came in December of 1982 when a data protection bill was submitted to the House of Lords (Jay and Hamilton, 1999). The progression of this bill was halted, though, by the 1983 general election. A second bill was submitted in July of 1983. This bill was passed the following year and enacted as the Data Protection Act of 1984 (Carey and Russell, 2000).

The Data Protection Act of 1984 came about as a result of the United Kingdom's desire to conform to the European Union legislation. This legislation required data users to register with the Data

Protection Registrar (DPR). It also introduced criminal offences for failing to comply with the regulations. Largely derived from the ten principles suggested by the Younger Committee on Privacy, the 1984 Act focused on eight key principles:

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes.
3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
4. Personal data held for any purpose or purposes shall be adequate, relevant, and not excessive in relation to that purpose or those purposes.
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7. An individual shall be entitled—
    a. at reasonable intervals and without undue delay or expense—
        i. to be informed by any data user whether he holds personal data of which that individual is the subject to; and
        ii. to access to any such data held by a data user; and
    b. where appropriate, to have such data corrected or erased.
8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.
   (Carey and Russell, 2000, p. 4)

One of the largest inadequacies of this Act was that it contained no requirement to comply, but only consequences for non-compliance. Many organisations are unlikely to comply with the legislation if not required, as it is costly and untimely.

In the 1990's, the British Parliament decided that too many loopholes existed in the 1984 Act and that it needed to be revised. As a result, the Data Protection Act of 1998 was drafted and enacted in March 2000. In addition to revising the eight key principles of the 1984 Act, the 1998 Act incorporated six features:

1. *Manual processing* – Subject to the operation of transitional provisions in the legislation, the 1998 Act applies to certain manual files as it does to automated data.
2. *Legitimacy of processing* – New conditions for processing exist as minimum threshold requirements before processing may be lawfully undertaken.

3. *Sensitive data* – A new category of personal data has been created. Sensitive personal data may not be processed unless one of a set of certain pre-conditions is satisfied.
4. *Data exports* – Transfers of personal data to countries outside the European Economic Area are banned unless certain conditions are satisfied.
5. *Data security* – Data may not be processed unless that processing complies with new security requirements.
6. *Individual rights* – Significantly more and stronger rights for individuals exist under the new legislation including the right to compensation for damage or distress caused by unlawful processing.
(Carey and Russell, 2000, p. 6-7)

Since the Data Protection of 1998 was enacted, numerous amendments have also been made to address problematic issues as they arise. As new forms of data storage and transmittance are developed (i.e. e-mail, internet registration), new adaptations are made to include them. This allows for flexible and effective legislation.

2.4 Data Protection Act of 1998

The 1998 Data Protection Act extends its definitions over the 1984 Act to include (with certain exceptions) paper-based filing systems, card indexes and other non-electronic collections of data (DPA 1998). The new Act went into effect March 1, 2000. Any new data that are collected are now liable to this Act; however, there is seven a clause in the Act for a "transition period" such that all data collected before March 1, 2000 has 7 years to come under compliance. There are eight principles that Data Controllers, those that oversee data storage and processing, must follow. Each of these eight principles is designed to ensure that personal information cannot be misused in any way.

2.4.1 Eight Principles of DPA and Applications

Each of the eight core areas apply to different sections of personal information protection, including storage, access, and transfer. The heart of the Act itself revolves around these eight principles, with the rest providing clarification.

2.4.1.1 Fair and Lawful Process

The first principle of data protection states that all data must be fairly and lawfully processed. Processing occurs whenever any operation or set of operations is carried out on a set of data. Therefore, whenever processing happens to that data, it must be done fairly and lawfully. In order for data to be considered handled "fairly and lawfully," it must uphold to one of a series of guidelines.

Fair and lawful processing entails the notification of the data subject (the person whose personal data are being processed) by the data controller to inform the individual that his or her data are being accessed. After this, at least one of the following regulations must be met in order to comply with the 1998 Act:

1. The person must give consent to the data controller for the processing of the data.
2. Processing of the data must be necessary in order to contact a person for consent.
3. The data controller is legally obligated, through whatever means, to process the data.
4. In order to better protect the data subject's personal privacy or interests, the data must be processed.
5. The data must be processed so that a public function may be carried out.
6. Processing is necessary to pursue the justifiable interests of the data controller himself, or some third party.

2.4.1.2 Processed for Limited Purposes

The second principle states that "personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes" (DPA 1998). The intent of this principle is to ensure that data are processed for limited purposes. This means that a data controller must not only notify a data subject when data are being processed, per guideline one, but also the extent of processing and to whom that data are being given. The reason for limited processing and notification is to ensure that personal data are transferred only after a data subject is initially informed, and then only used for purposes agreed upon by the subject. For example, if a company transfers customer lists to another company, a subject must be

informed of that transfer, as well as informed of the intended use of the information by the receiving company.

2.4.1.3 Data are Relevant and Not Excessive

This guideline is very specific in its interpretation. It states that an appropriate level of information should be stored concerning data subjects. This is to ensure that data controllers store only information that are relevant and discard any irrelevant or excessive information about data subjects. For example, for purposes of a mailing list, a person's date of birth is not required, and therefore would be considered excessive in this set of data. In certain instances in which more information is needed for any one individual, care should be taken to insure that such levels of data are not collected for all subjects. This guideline prevents personal information from getting stockpiled in databases, and prevents against the possibility of its improper use.

2.4.1.4 Accurate Data

Guideline four seeks to ensure the accuracy of private information. If personal information is being stored, accessed, and transferred, it is necessary that the information be accurate and up-to-date, so that the data may be used in the most positive way. There are some important aspects of this guideline that must be considered by data controllers. The importance of the accuracy of certain types of information must be assessed by the data controller, on the basis that its inaccuracy causes distress to the data subject. For example, a data controller might deem that it is more important for someone's address be listed correctly, then their current approximate salary. Also, the collection methods of the personal information must be acknowledged. Some questions to keep in mind are the validity of the source, how difficult it is to check the validity of the information, and the consistency of the method of data entry. The importance of this guideline is that if a citizen's personal data are being used for something very important, the data should be correct to protect against potential distress or injury.

2.4.1.5 Data are Kept no Longer than Necessary

Another important point addressed by the Data Protection Act of 1998 is that processed personal data be kept only for the amount of time that is necessary. Private information should only be retained as long as it is applicable. For example, information relating to specific legal cases should only be retained for as long as the governing statute remains active. A guideline such as this one requires that data controllers regularly review the data in their possession to ensure its relevance, while at the same time protecting data subjects from unnecessary and lengthy storage of their personal information.

2.4.1.6 Processed According to Data Subject Rights

Principle six states that data shall be processed according to the rights of the data subject under the 1998 Act. In essence, it is the all-encompassing rule ensuring that data are processed under the conditions specified in Part II of the DPA 98. For example, a data controller must ensure that personal information is not transferred for use in a direct marketing campaign, in order to comply with Section 11 of the DPA 98. The rights of data subjects can be found in Part II, sections 7 through 15 of the DPA 98.

2.4.1.7 Data are Secure

The seventh principle states: "Appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to, personal data" (DPA 1998). This means that data should be secure. This principle covers a broad range of activities, and includes both "technical," meaning physical, or computerised protection, and "organisational," meaning procedural or labour arranged precautions. A technical measure, for example, might be virus protection software installed on computers storing data and other precautions to prevent computer hacking and break-in. Organisational measures might include proper training of all employees involved in data protection regarding the DPA 1998, or ensuring that paper waste containing personal information is destroyed by a reputable contractor. There are many safety

measures that may be installed by a data controller to ensure the security of personal information, and the purpose of this particular guideline is to hold them responsible by law to set up such measures.

2.4.1.8 Adequate Protection for Transfer between Countries

The final principle of the Data Protection Act of 1998 ensures that any private information that is transferred to countries that are not members of the European Union is adequately protected. This guideline is particularly relevant to information that is posted on the World Wide Web. If a company or organisation posts private information on a website that is accessible from countries not within the EU, and is not adequately protected, then that organisation may be in violation of the DPA 98. This principle is also important to information in transit to all countries, especially those where levels of either physical or computerized protection are not in place.

2.4.2 Exemptions

With possession of personal information comes much responsibility. Even though some people might think that their personal information is their own, and completely under their control, there are certain instances when the right of privacy might be waived or adjusted. The Data Protection Act of 1998 contains a series of these exceptions, which are outlined in Part IV.

One area of exemption involves matters of national security. The United Kingdom's organisations and officials of the MI5, the Ministry of Defence and the Queen are exempt from the DPA 98. These organisations and persons all deal in matters where free and easy access to citizens' private information is crucial to the government's everyday operation. Any organisation that deals in matters of national security may also apply for a Certificate of Exemption, the details of which are thoroughly outlined in the 1998 Act.

As stated in section 29 of part IV of the 1998 Act, personal data processed for prevention and detection of crime; apprehension or prosecution of offenders; or the assessment or collection of any tax or duty are exempt from data protection. Therefore, any data relating to criminal cases, tax evasion, or other criminal investigations are accessible to the respective officials in search of such information. This exemption is quite similar to that of national security, but deals more specifically with legal and monetary issues.

The next areas that are exempt from the Data Protection Act are those of health, education, and social work. Per section 30, personal data consisting of information as to the physical or mental health or condition of the data subject is exempt of protection to the appropriate officials, such as emergency response personnel. Also, matters concerning educational grading on examinations are exempt to the appropriate individuals as well. Lastly, exemptions are granted for the correct carrying out of social work. The rest of the exemptions concern areas of literature, journalism, art and research. If any of these areas are of public concern, and do not relate directly to individual private information, they also are exempt from DPA 98 standards.

2.4.3 Enforcement

Part V of the Data Protection Act of 1998 describes the enforcement of its rules and regulations. The nature of this Act, the protection of personal privacy, requires that there is some amount of enforcement. The first clause deals with enforcement notices and describes how data commissioners can inform data controllers to perform some sort of operation on a piece of data. Section 42 says the following about requests for assessment:

> A request may be made to the commission by or on behalf of any person who is, or believes himself, to be directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act. (DPA 1998)

The purpose of the subsection is to empower data subjects with certain rights that allow them to access and know the private information that is being stored about them. The remainder of part V deals with information notices, special information notices, failure to comply with notices, rights of appeal, and powers of entry and inspection. Details on these sections can be located in the 1998 Act itself.

2.5 Conclusion

Data protection is the security of individuals' personal information. This information may consist of such data as a person's phone number, financial status, or legal history. The improper distribution of this sort of information may bring about severe negative results in an individual's life. Since it is crucial for people to retain a sense of privacy and security, it is imperative that their information is accessed, stored, and processed with care.

When an individual has access to personal information, he or she has the responsibility of treating that data with utmost caution. In order to ensure that this happens, many technologically advanced countries worldwide have instituted regulations for personal data protection. For example, the United States currently uses a constantly changing piece of legislation that was first passed in 1974. Likewise, the European Union utilises doctrine from 1995, based on principles developed in 1980. The United Kingdom similarly uses a 1998 revision of their 1984 Data Protection Act. All three of these governments supplement their primary legislation with amendments as needed.

When an individual wishes to ensure compliance with any type regulations, it is important to look at the aspects that influence compliance. In corporate cases, employers and managers must assess the reasons for which their subordinates are not complying. Then they must determine a method for

rectifying this lack of conformity. In most cases they choose to train their employees in the areas of non-compliance.

In this specific case, the London Borough of Merton (see Appendix A) is looking to improve its employees' awareness, and thus compliance, with the Data Protection Act of 1998. This is the governing piece of legislation concerning personal information security in the United Kingdom. It protects data kept on any living individual. It is summarized in eight principles. These principles state that a person's information must be accurate, secure, and stored for a limited time. In addition, data are required to be processed fairly and for limited purposes. Lastly, individuals have the right to request access to their own information.

These concepts and regulations are intended to protect the UK's citizens and make sure that their information is well protected. The London Borough of Merton realises that its employees' knowledge and implementation of these points are crucial. Furthermore, extended education and training of the workers at the Borough of Merton will enable them to comply thoroughly with Data Protection regulations. Thus the employees at the Borough of Merton will be able to provide personal information security for the citizens whose data they hold.

Chapter 3 – Methodology

The London Borough of Merton as a whole was not complying satisfactorily with the Data Protection Act of 1998. Thus, our sponsor deemed it necessary to evaluate the awareness levels among the members of the borough. Our group conducted interviews with members of the management to establish the current methods of training, as well as the effectiveness of those methods within each department.. The secondary purpose of the interviews was to develop surveys. These surveys evaluated the employees' awareness and perceptions of the Data Protection Act. From the analysis of this data we created recommendations for training plans to enhance awareness in each department. A timeline for the implementation of our methodology is presented in Appendix B.

3.1 Interviews

The interview process of this project was necessary in order gain insight into managers' perceptions of Data Protection Act compliance. Interviews allow individuals to "impart large masses of information about themselves" (Ackroyd and Hughes, 1992, p. 102). This procedure was divided into two different sections. The first part was an interview with our liaison, Mr. Simon Guild. One of the main purposes of this interview was to identify the project needs of the London Borough of Merton. In the second phase, we interviewed members of the management. This helped us to establish surveys as well as draw conclusions about the needed education plans.

3.1.1 Liaison Interview

On 14th January 2003, we met with Mr. Simon Guild, the Data Protection Officer, to gain a clearer understanding of the scope and expectations of the project. The interview questions are included in Appendix C. He provided us with a primary definition of the problem to be addressed. We asked Mr. Guild for a description of the organisational structure of the London Borough of Merton. He also provided us with eight individuals in higher-level managerial positions to interview. The information

from these interviews was used to create precise and appropriate survey questions, which are discussed in section 3.2.

3.1.2 Management Interview Guidelines

In preparation for the management interviews, we developed an interview guide (Appendix D). It was important that interview guidelines were "used consistently with the same meaning with all the respondents" (Keats, 2000, p. 75). This aided in maintaining the consistency of the material covered in each of the eight interviews, and ensured that all necessary areas of data collection were included. However, the interview guides were not completely rigid, and interviews still maintained personal flexibility in questioning (Keats, 2000). This provided the freedom to pursue lines of information that proved promising. Thus, we were able to focus on questions that were more relevant in a specific department.

The questions included in the interview guide were designed so that "variables under consideration were isolated" (Keats, 2000). First, we wished to know a brief description about their job occupation and how the managers' departments used the Data Protection Act. For this reason, we asked them how the Data Protection Act of 1998 had changed procedures in their department. Secondly, each interviewee was questioned about past methods of training used in their department. We further ascertained which of these methods were effective and well received by employees. This information was one of the main sources of information used to develop our recommendations. It was important for us to know which educational systems were likely to be useful when conveying information about the Data Protection Act of 1998.

Next, we wished to gain knowledge of the data protection measures currently in place in each department. In order to do this, we generated questions that concentrated on each of the eight data

protection principles. These questions were worded in common English to avoid a sense of testing and confusion caused by legal jargon. They allowed us to determine what areas of the Data Protection Act were lacking without asking the manager about his or her lack of knowledge.

We ended each interview by asking the managers what they would like to see on the survey. The purpose of this was twofold. First, we wanted to know what they wished to know about their staff. This indicated areas they felt were problematic. Secondly, we wanted to ensure the interviewee that his or her information was valuable to us and that it would have an immediate effect.

Before conducting each interview, we obtained consent forms from each individual interviewed. A sample form is included in Appendix E. The consent forms ensured that those interviewed had agreed to the method of collection, storage and usage of the data obtained during the interview. In addition, the consent forms verified that information collected was kept confidential. Individuals may be hesitant to answer questions indicative of their awareness of national legislation, as it suggests a level of knowledge, or lack there of, regarding data protection regulations. As this reluctance may have a debilitating effect on efforts to obtain useful information, consent forms were provided to put interview subjects at ease, knowing that their confidentiality was ensured. As a result, a higher level of accurate and relevant information on awareness and compliance was obtained (Berg, 2001).

Each set of interview questions was customised depending on the job description and position of the interviewee. An important idea we tried to convey to the subjects was that they were not being assessed on past mistakes. However, we wished to understand their current state of knowledge so that they will be more informed in the future.

3.1.3 Management Interview Procedures

All four team members were present for each interview. As suggested by Keats (2000), two team members conducted each interview, while the other two took written notes. During this interview process, we used a recording device. Taping the interviews on cassette allowed our team to more effectively focus on appropriate questioning and discussion without concern of missing information. It permitted us to maintain a complete record of each interview, and was used in conjunction with the written notes. Immediately after each interview was analysed and summarised, the tape was erased to ensure that the interview contents were not heard by individuals outside of the project team.

3.1.4 Interview Data Analysis

Following each interview, the group created an interview summary based on the recording as well as the written notes. This summary was produced immediately after the conclusion of the interview to prevent important points from being forgotten (Keats, 2000).

The interviews were not transcribed word-for-word. It was imperative that we not keep unnecessary records of the interview contents, due to the anonymity guaranteed to the interviewees. Thus, we only wrote down the information that was comparable to other interviews and useful for development of content and delivery of educational plans. Notes from these interviews are included in Appendix F. To ensure that vital information was not missed, we established a set of codes that were used for the classification of data. Codes were determined according to key words that signified importance to training methods and Data Protection Act compliance (De Vaus, 1991). Codes were established for a large range of possible responses, although a smaller range was found to exist (Keats, 2000). Furthermore, the standardization of interview guidelines allowed for the comparison of corresponding responses. Then we classified data according to our set of codes.

3.2 Surveys

The government of Merton has requested a measure of the level of awareness within their division. We distributed surveys including a confidentiality agreement (Appendix G) within the departments of the Borough to determine awareness with the Data Protection Act. The survey was a powerful tool in determining the government employees' needs and how their level of awareness can be increased.

3.2.1 Survey Design

In the process of writing our survey, clear and concrete objectives were important, as they aided in determining what areas of data protection needed to be addressed. Due to the sensitive nature of the survey topic and the possibility of causing controversy, caution was a necessity when wording the survey questions. It is imperative that surveys "allow individuals to be interviewed about their…feelings, attitudes or beliefs without feeling unduly threatened, intimidated or insulted" (Ackroyd and Hughes, 1992, pg. 39). Thus, we formulated questions with the purpose of making the survey subjects comfortable enough with the questions to give an adequate and truthful answer.

While in the process of interviewing the managers (as described in section 3.1), we began designing our surveys. Two questions per survey were based on the information we obtained from those interviews. That is, after understanding the barriers to awareness of the Data Protection Act of 1998, it was possible to create surveys that targeted those problematic areas. However, the remainder of the questions covered all eight principles of Data Protection. This was done to ensure that the survey addressed dependent and independent variables, each department's specific needs, and all possible areas of knowledge (De Vaus, 1991).

Our surveys kept anonymity and posed straightforward, concise questions as recommended by De Vaus (1991). They were designed with the intention of obtaining information about the employees'

work practices with respect to data protection. This implies that questions were not "double-barrelled" or leading (De Vaus, 1991, p. 49). In addition, we aimed to learn about individuals' perceptions of the Data Protection Act and its implementation.

3.2.2 Survey Format

There were five different surveys. A separate survey was designed for each of the five departments in the London Borough of Merton. Each survey began with a disclaimer that assured the respondent of his or her confidentiality and explained the use of the information he or she provided. Following this, our survey was separated into sections. It can often be helpful to divide the questions into different types. These can be classified as "behaviour, beliefs, attitudes, and attributes" (De Vaus, 1991, p. 81). In our survey, the "beliefs" and "attitudes" sections were combined.

The first survey section was designed to address the "attributes." It was the same for each of the five surveys. Here we asked the respondent to give us his or her department name. In addition, we requested that the respondent defines his or her position as managerial or non-managerial. We formulated these two questions to aid in the categorization of analysed data. It was important for us to know the levels of awareness and areas of misunderstanding within each department in order to develop individual educational plan recommendations. In addition, given the tiered organisational structure of the London Borough of Merton, it was necessary to know the respondents' managerial level. This allowed us to evaluate the amount of information that is distributed to each level of management. We did not ask for the respondents' exact tier level, as this would have revealed the identity of upper-level management. Other questions in the first section were short questions about respondents' training and experience with data protection. These were included in the first section due to their universal application to all five departments.

The second section of the surveys was different for each of the five departments. This part consisted of a set of two hypothetical situations. This section contained questions that can be described as "behavioural." In this part, a short scenario was described. Following this narrative, the respondent was asked what he or she would do. Each set of cases was designed to target the problems observed in each department. The information needed to develop these scenarios was gathered from the interviews with the management of each department. In addition, the Data Protection Officer's concerns and recommendations were taken into account. The scenarios evaluated the respondents' ability to correctly deal with problematic situations that could arise in their daily work.

The final part of the surveys was focused on "beliefs" and "attitudes." This section evaluated the feelings of respondent about data protection. We asked the respondents to rate their level of agreement with a set of statements. The aim of this was to determine whether respondents perceived the Data Protection Act of 1998 as necessary, effective, and worthwhile. This was important, as employees may be incompliant with rules for various reasons. Even if they are aware of regulations, they may disregard those they deem excessive or irrelevant.

3.2.3 Survey Details

A primary concern when developing a survey is selecting a proper sample size. A suitable sample size is important to acquire adequate and accurate information. At the same time, we had to be careful with the sample size because too many individuals would have resulted in an overload of data, hampering analysis efforts. It was important to select people within the organisation who would provide the most relevant information. In order to obtain a representative sample, we provided all workers at the London Borough of Merton Civic Centre the opportunity to complete the survey.

Our sample consisted of the approximately 2500 managers and subordinates at the Civic Centre. In addition to the need for all employees to be offered a chance to submit the survey, we chose a large sample size due to an expected 25% response rate. Similar online surveys recently conducted at the London Borough of Merton have received comparative response rates (Burke, 2003). Surveying 2500 employees ensured a satisfactory amount of information to analyse, considering the large number of individuals expected not to respond to the survey. The large sample size helped us obtain sufficient and relevant data to further determine the barriers to compliance.

Another issue was determining how to maximize the survey response rates. Effectual survey methods, timing, and incentives were all essential factors in developing the surveys (Guild, 2003).
The surveys were also anonymous, short and concise so individuals were able to complete them within a ten-minute time period. The most prominent incentive included in our survey process was a raffle (Burke, 2003). The survey was web based (see Section 3.2.4), therefore a counter was installed at the bottom of the survey web page. Once the respondents were finished with the survey, they e-mailed the number from their survey to our team. The number served as a confirmation that they had actually completed the survey. We assured the respondents that this number was not in any way used to link their responses to their identities. Numbers were then entered into a drawing for several prizes.

3.2.4 Implementation

Our survey was conducted online. Our group decided to utilize this method due to the anticipated higher response rate. We expected that the ease of answering a survey online as compared to filling out a paper survey would result in a greater amount of replies.

We used Perseus, an online survey tool, to implement our survey. Using this program, we created five different websites. Appendix H shows an example of the online survey template. Appendices I - M show the questions that were asked for each of the five departments. Each website contained one of the department-specific surveys. After posting all of the surveys, we sent the links to these websites. The IT Services forwarded the links to all the employees within the London Borough of Merton via a global e-mail. The link from the Perseus survey was distributed the 30th of January. Those that completed the survey by the 31st of January were entered into a drawing for three vouchers for Borders Bookstores. One of these vouchers was for £20 while the other two were worth £5. Each respondent was eligible to win only one of these prizes. An e-mail reminding employees to respond to the survey was sent out the 4th of February. Employees who replied by the 6th of February were eligible to win one of the two £5 vouchers. All three winners were notified via e-mail the 7th of February.

There were several aspects of our survey's delivery that proved problematic. First, there had been several surveys done shortly before ours at the Civic Centre. Employees had thus become tired of surveys. In addition to this, global e-mails historically have a low response. Therefore, when e-mails were sent out to the employees, the subject shown on our e-mail was very important to our response rate. It was imperative that employees' interest be piqued by this subject in order that they not delete the e-mail upon observing its sender. Because of this, we were careful to avoid the word "survey" in the subject box. In addition, we composed an eye-catching phrase to grab the reader's interest. However, due to miscommunications between our group and IT services, the subject box of our first e-mail announcing the survey was left blank. Likewise, the reminder e-mail, sent on the 4th of February, contained the subject "Data Protection Survey." We believe this affected our response rate significantly. We received 242 by the deadline with a 13% response rate.

3.2.5 Analysis

Perseus e-mailed sets of results to our account in groups of twenty-five. These data sets were separated into groups according to their respondents' department. Further, they were divided into objective and subjective questions. Once survey data were collected and categorized, we examined the objective questions. First we examined the overall percent of correct answers. These data informed us of the necessity for an educational plan in each department. They also allowed us to foresee possible complications in the creation of each plan due to large disparities in individuals' present knowledge (Guild, 2003).

Next, the objective results were categorized by question and the percentage of correct responses per question was evaluated. We calculated this in order to understand the areas that presented problems in each department. This would serve to indicate whether knowledge was lacking in data protection as a whole, or only in concentrated areas. Survey results are included in Appendix N. When developing our recommendations regarding the education plan, these results enabled us to determine the areas of focus for each department.

Chapter 4 – Results and Analysis

After conducting our surveys and interviews, we analysed the information through qualitative and quantitative measures. Survey results and survey coding are shown in Appendices N and O respectively. There were two main factors that were examined in order to formulate data protection training recommendations. First, we considered data protection awareness among employees at all levels to determine the content of the proposed educational plan content. Following this, we examined the information describing training and compliance. Using this data we determined the best manner or manners in which to deliver the department educational plans.

There were varying survey response rates within different departments in the London Borough of Merton (see Table 1). In the Education, Leisure and Libraries, 39 of 480 (8%) of the department's employees responded to our survey. Results were similar in the Environmental Services, with 31 of the 318 (10%) employees replying. However, response rates ranged between 12% and 23% in the Finance; Housing and Social Services and Chief Executive departments. We believe that these differences in response rates are due to the various levels of contact that each department has with personal data. For instance, the Housing and Social Services department has access to large amounts of sensitive information. However, the majority of employees in Environmental Services and Education, Leisure and Libraries' Services do not hold large amounts of sensitive information. Therefore, we feel that the employees in these departments may have been less inclined to reply to our survey as they may have felt that it had little to do with their jobs or job specifications.

Table 1. Survey response rates

Department	Number of employees	Number of respondents	Percentage
Chief Executive	385	57	15%
Housing and Social Services	350	80	23%
Finance	293	35	12%
Environmental Services	318	31	10%
Education, Leisure and Libraries	480	39	8%
Total	**1826**	**242**	**13%**

4.1

Awareness and Compliance

To begin our analysis, we first evaluated employees' awareness of the Data Protection Act of 1998. This included individual knowledge and departmental procedures as well as employees' perceptions. It was important to determine the subordinates' views of the regulations when examining and comparing awareness and compliance. Therefore, we also analysed their opinions of data protection importance and effectiveness.

4.1.1 Chief Executive

Two members of the London Borough of Merton's Chief Executive management were interviewed. In these interviews, one manager mentioned that employees were generally aware of the Data Protection Act of 1998, but did not have knowledge of the specifics of the act. The second manager stated that the levels of awareness between employees varied significantly. When we surveyed the employees about their awareness, 37 of 57 respondents (66%) described themselves as having "general awareness, but not of the details" of the Data Protection Act, as shown in Figure 1. Eleven percent said that they had in-depth knowledge of the regulations and thirteen of the 57 (23%) described themselves as "not really knowledgeable."

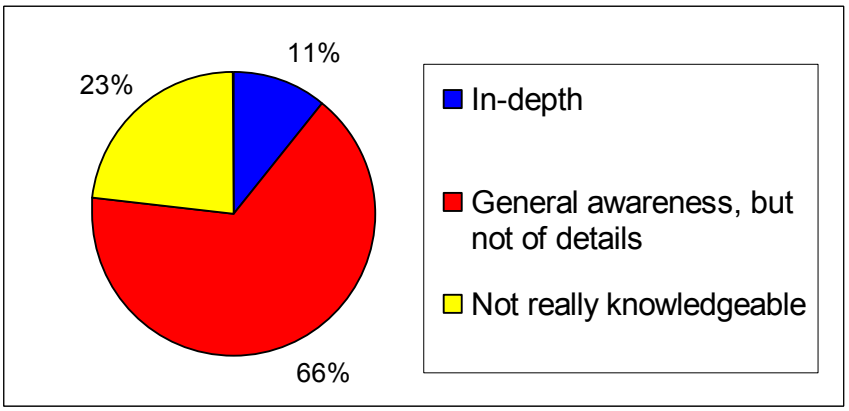


Figure 1. Description of Data Protection Act awareness in Chief Executive department

Both managers interviewed cited problems with the tracking of information. One manager said that there was a need for improvement regarding data tracking. The other manager stated that there was no way to track information. In addition, the second individual stated that there were many "casual records" kept by employees. In support of this, 20% of the employees surveyed in the Chief Executive department stated that they believed it acceptable to keep personal casual databases. Although 20% is not a majority, it represents a significant noncompliant section of the Chief Executive department.

Management interviews also revealed that there was no protocol for dealing with data subject requests. Both managers interviewed stated that a documented procedure for handling such requests was needed. It is our opinion that employees may not know how to handle data subject requests because there is no documented procedure. This lack of knowledge was further demonstrated in our survey results. As shown in Figure 2, eleven percent said that no repercussions would occur due to an unanswered data subject request. More than a quarter of respondents (26%) thought that the penalty for this mistake would be a verbal reprimand from a supervisor. However, the majority (72%) correctly responded that they were legally responsible for complying with data subject requests. Although most employees were aware of the consequences

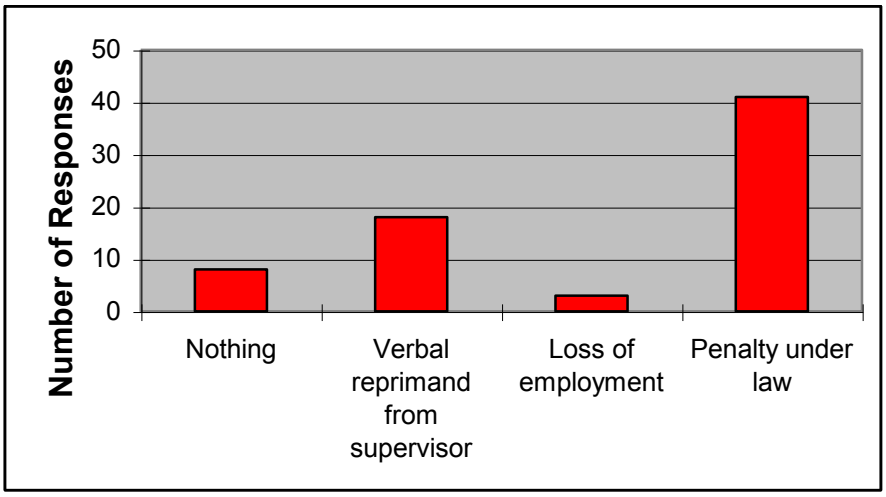


Figure 2. Perceived repercussions of non-compliance in Chief Executive department

of non-compliance, the fraction that believed there was no consequence at all composed a significant portion of the department.

In addition to the lack of data subject request protocol, the managers stated that data subject requests were not always taken care of within the specified forty-calendar-day period. Furthermore, the Legal Services manager interviewed said that a high number of requests would impair the department's ability to respond to a request in a timely manner. In order to evaluate the employees' knowledge on this matter, we asked how many days they felt were allowed to fulfil a data subject request. Survey results, illustrated in Figure 3, show that only four of the 57 respondents (7%) knew the appropriate time period (40 Calendar Days) for a data subject request reply. However, 44 respondents (82%) selected a period shorter than the mandated time. We feel that there may have been an inherent flaw in the survey question posed. Respondents may have chosen the shortest time period provided in order to ensure that they were within regulations.

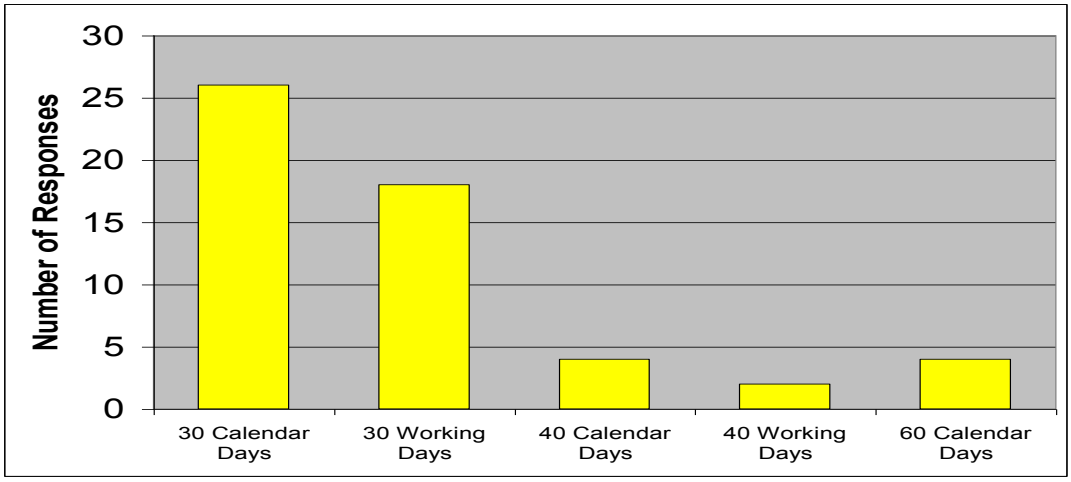


Figure 3. Perceived time allowance for data subject requests in Chief Executive department

Both of the Chief Executive managers interviewed stated that one of the most prevalent problems in their department was the fact that data is not kept up-to-date. Each interviewee said that an excess of information and lack of personnel were reasons for excessive and inaccurate data. Personnel were said to be too busy with other work to review and correct old files.

4.1.2 Housing and Social Services

One of the two interviewees from Housing and Social Services stated that their employees were aware of the general implications of data protection, but lacked knowledge of the specifics. The other said that employees were very aware of the Data Protection Act. This second person went on to say that employees such as social workers are trained in data protection in the university. When survey respondents described their own knowledge of the Data Protection Act of 1998, however, 24% said that they were "not really knowledgeable" (Figure 4). Most respondents, 73%, said they had general, but not in-depth knowledge. Only a small section (3%) of the respondents, described their knowledge as being in-depth.

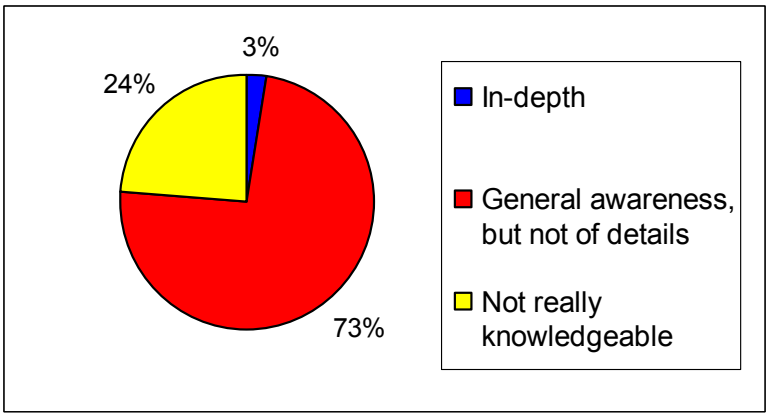


Figure 4. Description of Data Protection Act Awareness in Housing and Social Services

Given the quantity and sensitivity of data that is held in the Housing and Social Services department, response to data requests was an important area of research. Both managers reported that there was a procedure in place to deal with data subject requests. One manager said that the current protocol was under review. However, only four of the 80 survey respondents knew the Data Protection Act's regulatory response period for data request (40 Calendar Days), as shown in Figure 5. As in the Chief Executive department, the majority (76%) of surveyed employees selected a response time less than the specified time. In addition to being questioned about the response period allowed by the Data Protection Act of 1998, employees were asked how to respond to a data subject request including sensitive information. In this specific case, the parent of a child calls requesting information held on the child. There is sensitive data held on the child, including information about special education and potential abuse. As illustrated in Figure 6, about half (51%) would correctly give the parent part of the child's information. Slightly less than half (45%) would refuse information altogether. The remaining 4% of Housing and Social Services respondents said they would give the caller all of the child's information. This would include the identity of the individual who reported the potential child abuse to the London Borough of Merton.

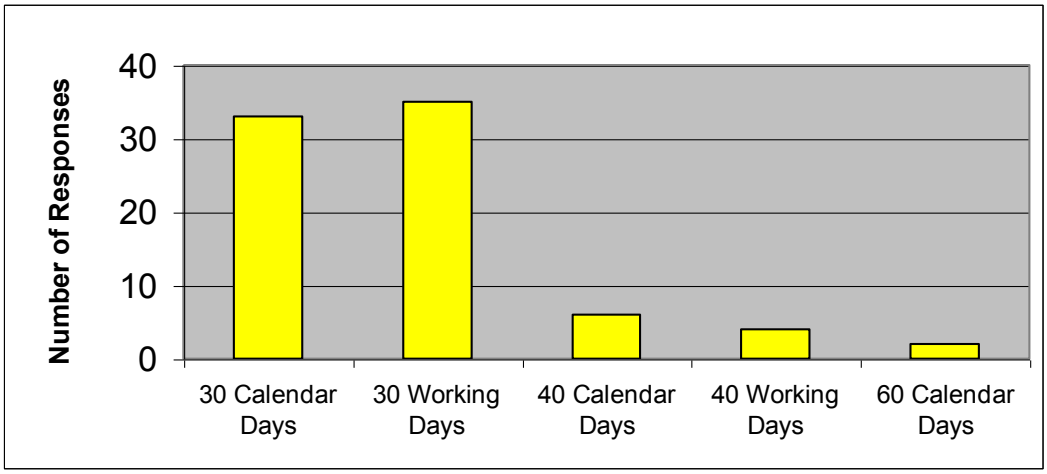


Figure 5. Perceived time allowance for data subject requests in Housing and Social Services

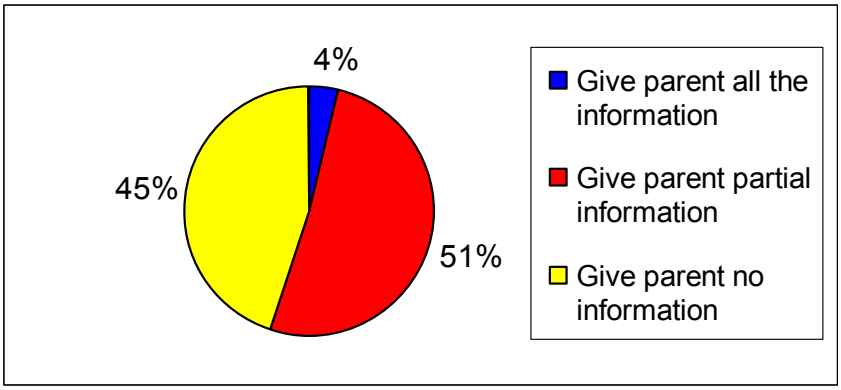


Figure 6. Data request containing sensitive information in Housing and Social Services

Employees were asked what would happen if an individual's data request was unanswered. Figure 7 shows that ten of the 80 survey respondents (13%) stated that there would be no repercussions for not replying to a request. Forty-seven respondents (59%) correctly responded that there would be legal penalties for non-compliance. Thirty-five of the 80 employees surveyed (44%) stated that a supervisor would reprimand them. However, this question allowed for multiple answers, so this does not necessarily imply that 44% of the employees feel that a verbal reprimand would be the only repercussion.

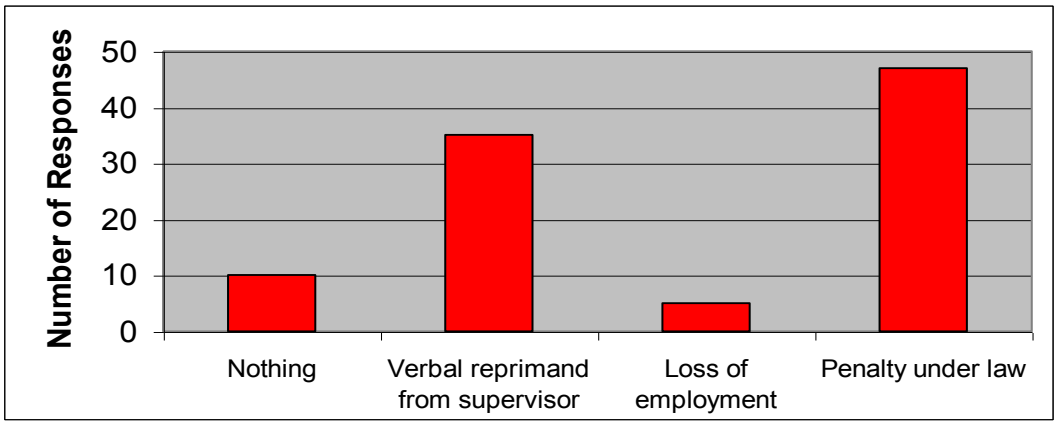


Figure 7. Perceived repercussions for unanswered data subject requests in Housing and Social Services

As in most departments, the issue of information accuracy was a concern. One manager indicated that data kept within the Housing and Social Services department was not up-to-date. This individual stated that there was no council-wide policy for maintaining accurate information, but one was needed. This interviewee indicated that a periodic case review was essential. The second manager interviewed stated that case files were updated at the beginning and end of each case, but did not indicate whether he or she felt that this procedure was adequate. Given the apparent problem with inaccurate information in Housing and Social Services, we wanted to find the source of this error. Therefore, we surveyed employees concerning the reasons for information inaccuracy. We created a hypothetical scenario in which they found an outdated file. We then asked what they felt was the most likely cause of this factual error. Forty-eight percent of the respondents cited improper file handling, while 37% named poor data protection training as the probable culprit, as shown in Figure 8. Fifteen percent, the smallest section of respondents, thought that lack of resources were the source of inaccurate information within files.

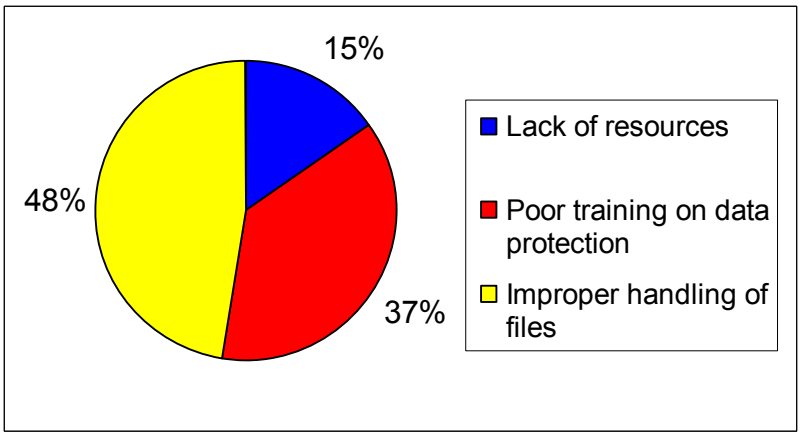


Figure 8. Perceived sources of inaccurate data in Housing and Social Services

4.1.3 Finance

One member of management in Finance was interviewed. This created some limitations regarding the reliability of data gathered from that interview, as we had no other interviews for comparison. The individual interviewed stated that employees within the Finance department complied with the Data Protection Act of 1998. This person cited severe consequences for non-compliance, such as job loss, as reasons for compliance in the department. The results of the surveys, however, contradicted department awareness levels cited in the interview. Although compliance and awareness are not synonymous, only two of the 35 respondents (6%) stated that they had in-depth data protection knowledge. The vast majority, twenty-eight of 35 respondents (85%) said that they would describe their awareness as general, but not detailed, and 9% described themselves as "not really knowledgeable." These results are illustrated in Figure 9.

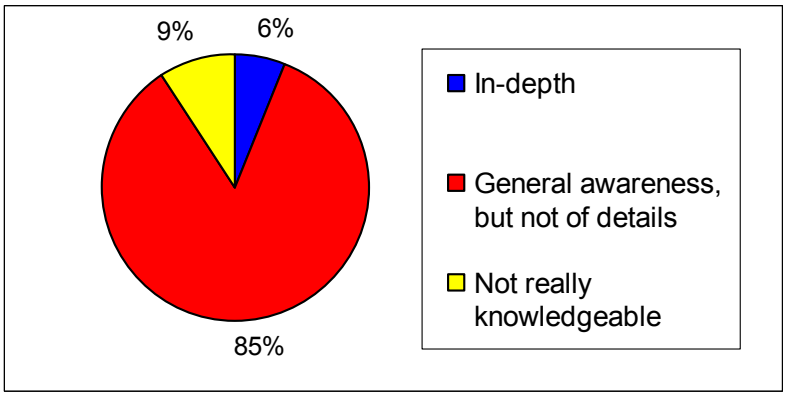


Figure 9. Description of Data Protection Act awareness in the Finance department

Our interview revealed that there is no protocol in place for the handling of data subject requests in the Finance department. As of the interview date, the manager said that no requests had been made. This interviewee stated that if an individual wished to see their data, there would most likely be an informal exchange of data via an appointment. Following this, employees within the Finance department were questioned about several aspects of data subject requests. First, we asked what would be the consequence of non-compliance with a data subject request. Multiple answers were allowed. Figure 10 displays that the majority, twenty of 35 respondents, correctly replied that they would be legally responsible. Six respondents thought that there would be no repercussions at all.

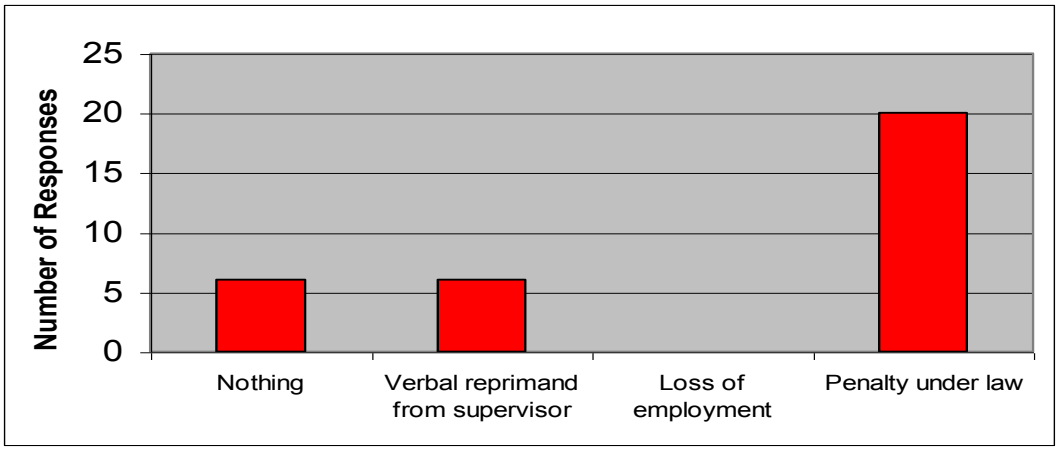


Figure 10. Perceived repercussions of unanswered data subject requests in the Finance department

We asked the manager if the department could fulfil data subject requests within the obligatory time period. The individual responded that such requests would probably be fulfilled within forty business days. However, the manager felt that if the information requested were too extensive, it might take longer to fulfil the request. In order to determine if employees knew the Data Protection Act's time regulations on answering data subject requests, we asked respondents how long they would have to comply with such a request. Only one of the 35 respondents was aware of the Data Protection Act's time mandate. As with other departments, the majority of respondents (58%) chose the shortest time periods (see Figure 11).

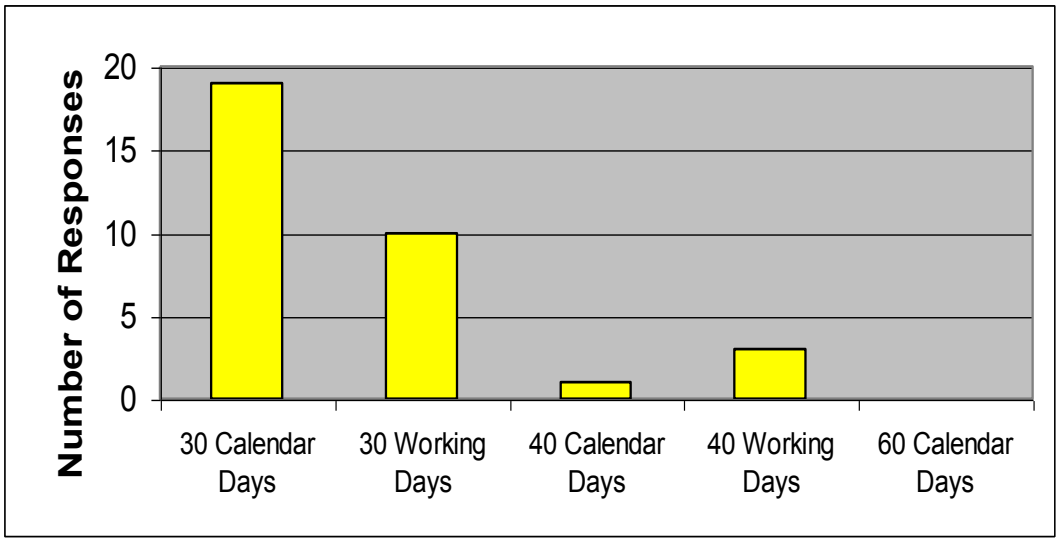


Figure 11. Perceived time allowance for data subject requests in the Finance department

4.1.4 Environmental Services

Two managers were interviewed from the Environmental Services department. Although both managers stated that employees lacked in-depth knowledge of Data Protection Act regulations, they cited different causes of this. The manager of one division said that data protection was not among

employee's priorities. This individual stated that data protection awareness was similar to environmental concerns in that employees were not worried about it. This was said to be due to the fact that they did not think it directly affected them and they were too busy with other work to be worried about Data Protection Act regulations. However, as Figure 12 shows, 57% of survey respondents in the Environmental Services department agreed or strongly agreed that following data protection regulations was as important as the rest of their work. Only 10% of employees stated that it was less important to follow the regulations than to complete other work. Furthermore, only five of the 31 respondents (16%) said that it took too much time to follow data protection regulations. The second manager from Environmental Services said that employees were not aware of data protection statutes because of insufficient clarity and legal jargon.

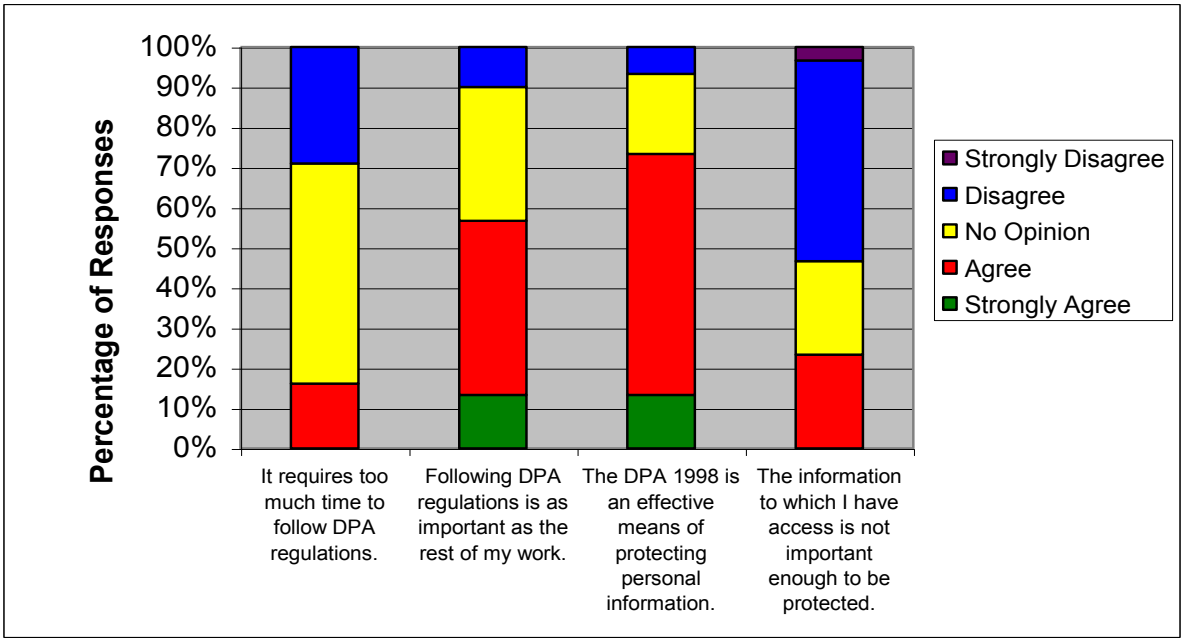


Figure 12. Opinions about Data Protection Act importance in Environmental Services

Each of the Environmental Services managers said that data security was one of the most predominant data protection problems in their departments. One stated that the department did not hold complete files, but only unofficial files with information given by other departments. Both managers said that

there was insufficient interdepartmental security. In our employee survey, we posed another hypothetical situation in which the respondent was asked by a member of another department to provide information about a client. As shown in Figure 13, 30% of the respondents replied that they would deny the employee all information, while 7% would provide all requested data. However, 63% chose the appropriate answer: they would provide only information that was deemed relevant to the other employee's purposes. In addition to interdepartmental security, one manager stated that files were kept after they were no longer necessary, and were often stored in insecure manners. Survey results supported this: 32% of surveyed employees said that files were kept indefinitely on their desks (Figure 14). Furthermore, in another question, nearly half (47%) of respondents did not know how to password protect a file on their computer, while 53% did.

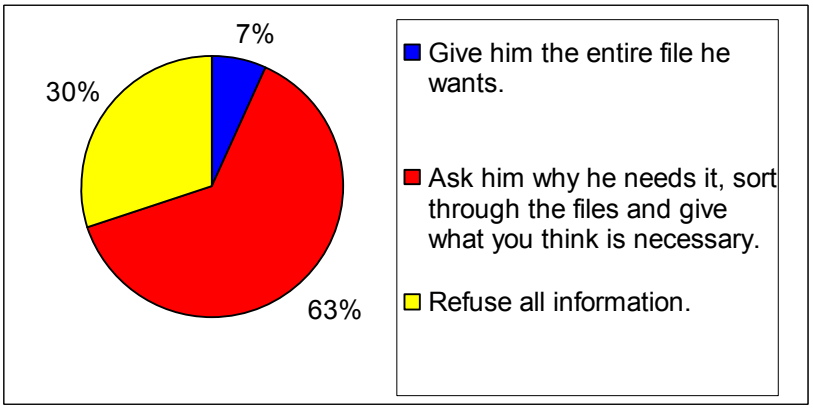


Figure 13. Interdepartmental data transfer in Environmental Services

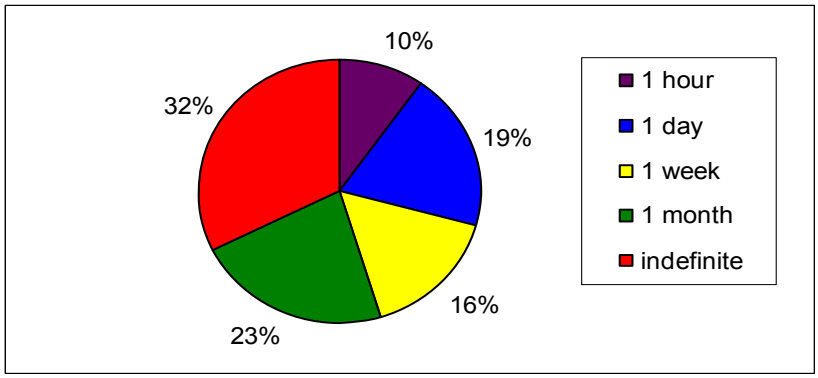


Figure 14. Typical time files stay on Environmental Services employees' desktop

4.1.5 Education, Leisure and Libraries

One manager from the Education, Leisure, and Libraries department was interviewed, providing the same dilemma as in Finance, as there was no other interview from the department as a basis for comparison. We asked the interviewed manager of Education, Leisure and Libraries what the average employee knew about the Data Protection Act of 1998. The manager replied that employees were aware of the need for data protection. However, as in many other departments, it was indicated that they were unaware of the specific implications of the Data Protection Act of 1998. The manager cited lack of knowledge and little training as the biggest obstacles to compliance. We then asked employees to rate their own knowledge of the act. Figure 15 shows that 61% of respondents believed they had general, but not detailed knowledge. Eight of the 39

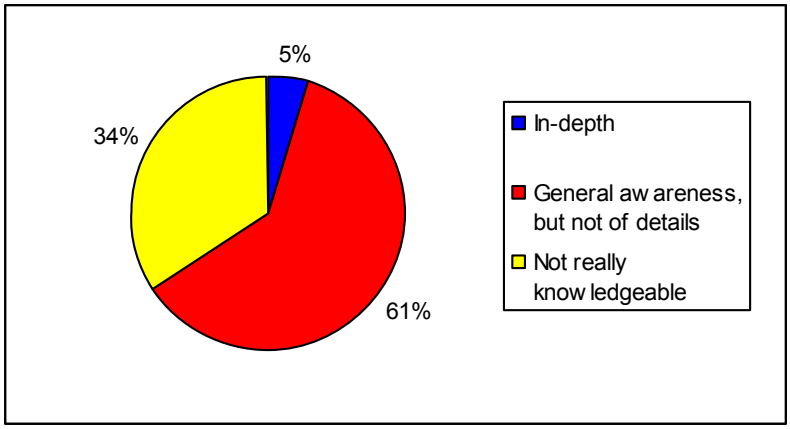


Figure 15. Description of Data Protection Act awareness in Education, Leisure and Libraries

respondents (34%) described themselves as "not really knowledgeable." Out of the five departments, Education, Leisure and Libraries was the one that had the largest majority of respondents said they were not really knowledgeable of the Data Protection Act.

We asked the manager whether there was any written procedure for dealing with data subject requests. The interviewee responded that most requests were dealt with by appointment, and that there was no documented protocol for handling these requests. In order to understand employees' knowledge of data subject request regulations, we asked them what would happen if a personal data request were unanswered. As Figure 16 shows, 10 of 39 individuals in the Education, Leisure and Libraries department thought that there would be no repercussions for this mistake. Twenty-one of 39 employees correctly responded that they would be legally responsible for this error. In addition to questioning employees about individuals making data subject requests, we asked them about the amount of information that should be revealed in the case of a data request about a third party. In this case, we created a hypothetical scenario where an employer calls requesting information on a job applicant. Twenty of thirty-eight employees, slightly over half, replied that they would not give this employer any information. Eighteen employees responded that they would inform the caller of the applicant's employment history. No respondents said that they would reveal the applicant's financial status or criminal record.

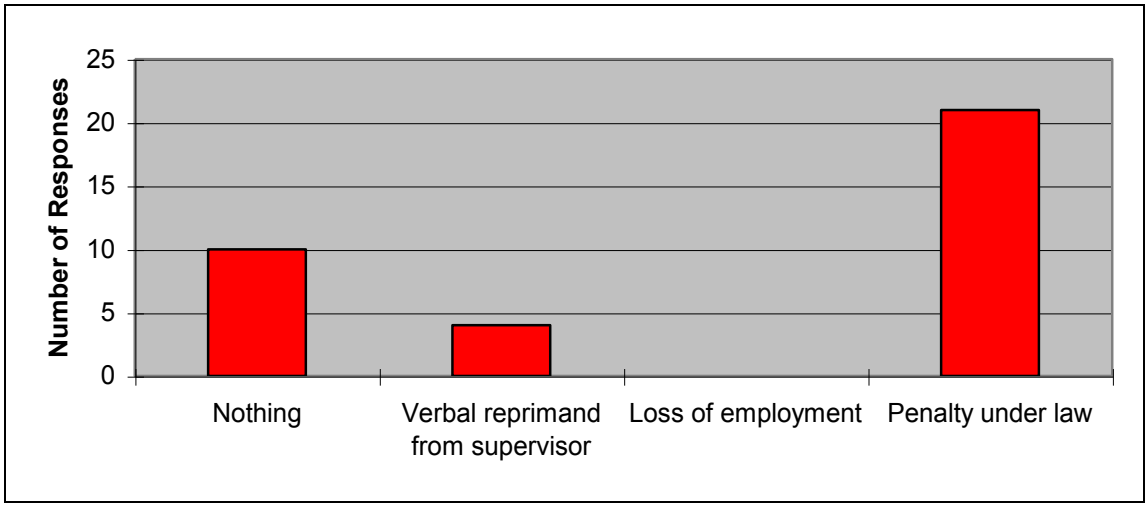


Figure 16. Perceived repercussions for non-compliance in Education, Leisure and Libraries

4.1.6 Common Results

There were several points that appeared repeatedly in the data, regardless of the department from which the information was obtained. First, it was found that in five of eight interviews conducted, the managers mentioned that their subordinates lacked specific knowledge of the Data Protection Act guidelines. They stated that employees within their departments were aware of the existence of the Data Protection Act of 1998, but were unaware of the specific regulations and the application of these rules to their jobs. Figure 17 shows that the employees share this view, as 161 of 242 respondents (73%) described themselves as having general, but not specific knowledge of the Data Protection Act. Twenty-one percent of employees rated themselves as "not really knowledgeable." This left fourteen of the 242 respondents (6%) as having in-depth knowledge of the regulations contained in the Data Protection Act of 1998.

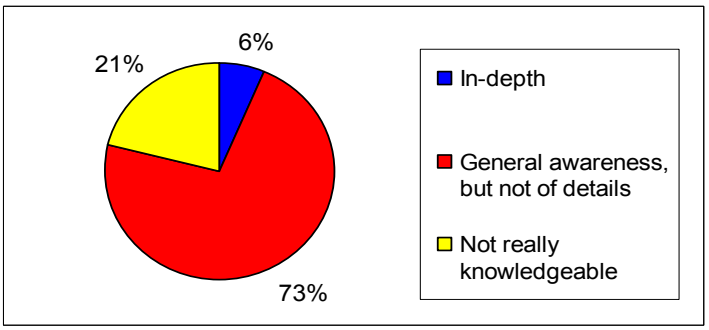


Figure 17. Description of entire Civic Centre Data Protection Act awareness

If managers mentioned a problem with Data Protection Act compliance in their department, we asked them what they thought were the major obstacles to compliance. Only one of the individuals said that the problem was due to a lack of concern on the part of employees. This individual also said that employees had too much other work, and did not see the direct importance of Data Protection Act compliance. The other managers we interviewed cited lack of specific knowledge as the foremost obstacle to compliance. We then asked employees about their opinions concerning data protection

importance. Figure 18 shows the responses of employees to different statements about the value and effectiveness of the Data Protection Act. As is shown, 68% of survey respondents agreed or strongly agreed that following Data Protection Act regulations was as important as the rest of their work. Only 14% of the employees stated that complying with data protection regulations took too much time. However, even though the survey was anonymous, we feel that employees may have given the answers that they thought we were looking for. Individuals may have been hesitant to tell a group working with the Data Protection Officer that they thought the Data Protection Act was not worth their time.

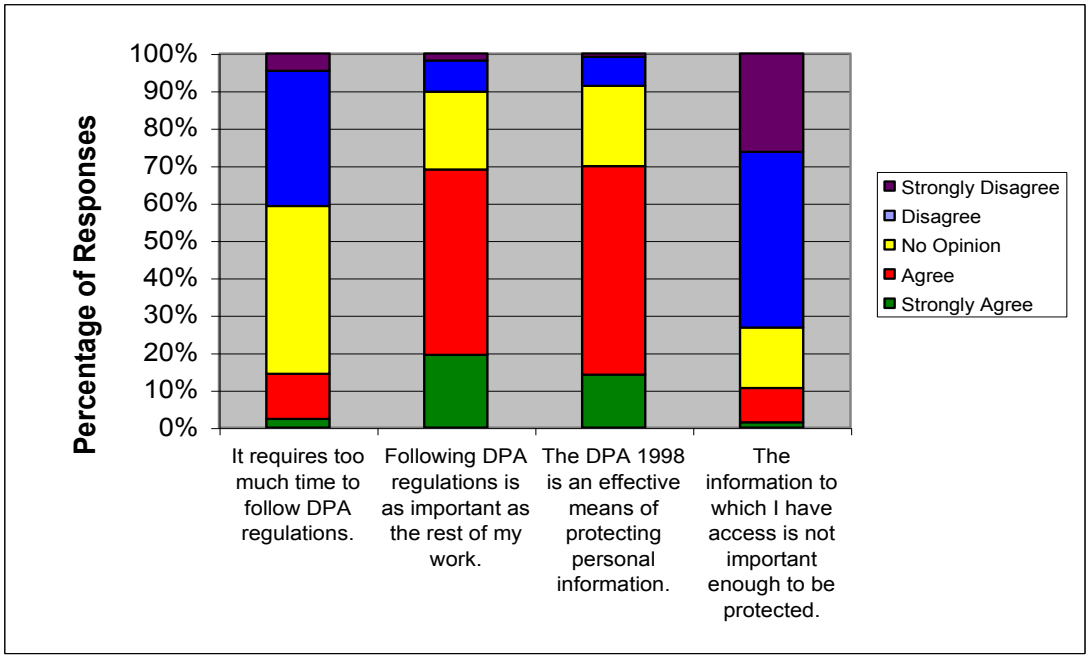


Figure 18. Civic Centre employees' responses to statements concerning Data Protection Act importance

Another issue was the handling of data subject requests. Seven of the eight managers interviewed stated that there was no documented protocol for dealing with these requests. However, four of the managers stated that they felt they would probably be able to comply with a request if one were presented. Two of these four felt that their department's ability to deal with requests would be adversely affected by a large volume of data subject requests or a complex request. However, when

employees were asked how many days were allowed to comply with data subject requests, only 7% chose the time frame dictated by the Data Protection Act of 1998. As in many individual departments, the majority (86%) of the London Borough of Merton employees selected the two shortest time periods available. These results are summarised in Figure 19.

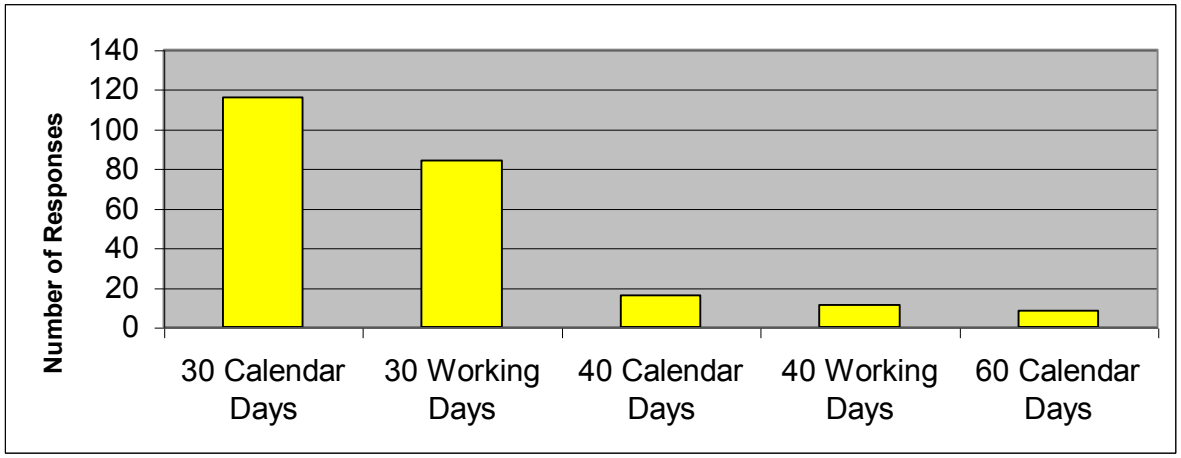


Figure 19. Perceived time allowance for data subject requests in the entire Civic Centre

One final factor repeatedly mentioned was that information held in each department was deemed to be out-of-date and excessive. Of the eight managers, seven stated that files held on individuals contain inaccurate data. These managers also felt that their departments possess data about individuals that is no longer relevant or necessary. However, not all surveys contained questions to verify this managerial perception. Therefore, we do not know if all employees share this opinion.

4.2 Education and Training

Our second area of analysis was training and educational methods. We studied past data protection training, current training methods, and employees' perceptions of different educational systems. First, we determined the current level of data protection training so as to know where to start with the proposed training plans. Then we established which methods were presently used in each department.

Lastly, we determined employees' perceptions of these methods in order to see whether or not current methods would be effective.

4.2.1 Chief Executive

One manager in the Chief Executive department stated that there was no current data protection training for employees. The other Chief Executive manager interviewed cited several "in-house" sessions as well as external courses, but continued to say that these were expensive. When employees were asked about their data protection training, 38 of the 57 respondents (68%) said that they had never been trained. However, ten of the 57 respondents (18%) said that they had undergone data protection training within the last six months. This can be seen in Figure 20.

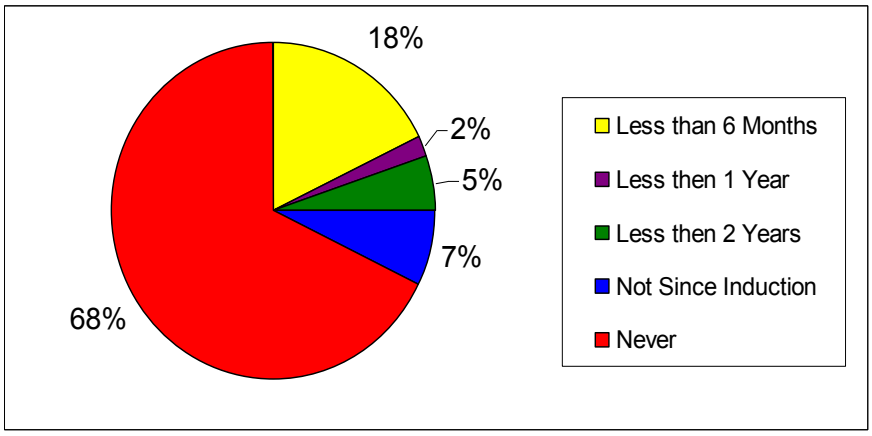


Figure 20. Time since last Data Protection Act training in the Chief Executive department

Team meetings were recommended as the best form of communication in the Chief Executive department by both interviewees. One manager recommended meetings with small groups and said reminders such as notice board posters should be given after the meetings. The other management member recommended that written regulations be presented followed by group discussion. Both recommended interactive group learning. Figure 21 shows the Chief Executive employees' opinions of these communications methods. Pamphlets were best received, with 56% of respondents listing this

method as "preferred." Work in team meetings received a moderate response, with a 36% approval rate. Posters proved to be the least liked with only 28% preferring them and 19% of the respondents disliking these reminders.

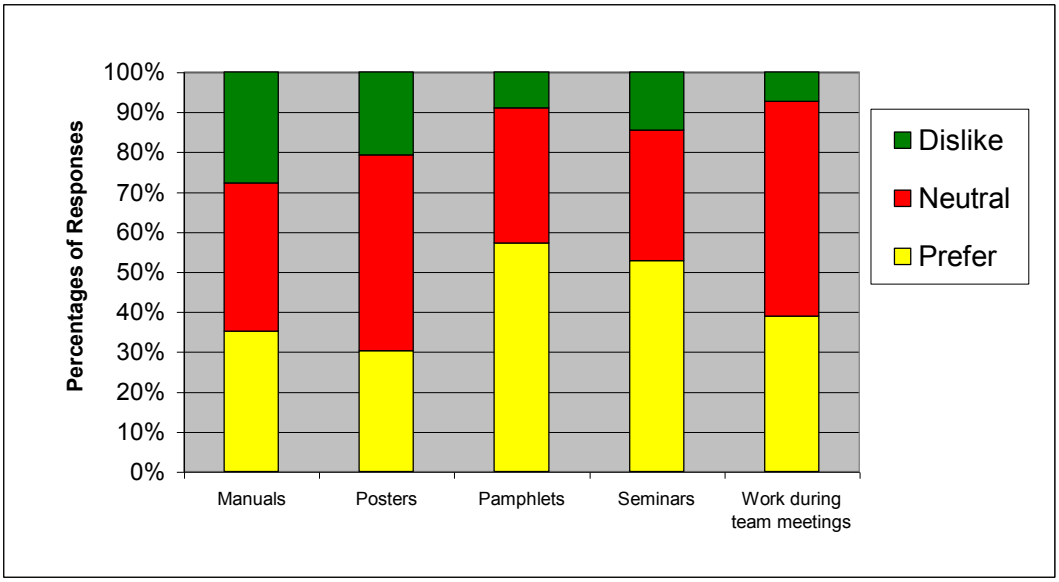


Figure 21. Chief Executive employees' opinions of various training methods

4.2.2 Housing and Social Services

Of the two managers interviewed from the Housing and Social Services department, both stated that their subordinates had data protection training. They specifically mentioned training on Caldicott standards although they cited Data Protection Act education as well. The Caldicott standards are a set of data protection guidelines adopted by Housing and Social Services. However, these are not legally binding. We asked survey respondents when their last data protection training occurred. Contrary to what was said in the interviews, 81% of survey respondents stated that they had never had any data protection training (Figure 22). Another 6% said that they had not been trained regarding data protection since their induction to the London Borough of Merton.

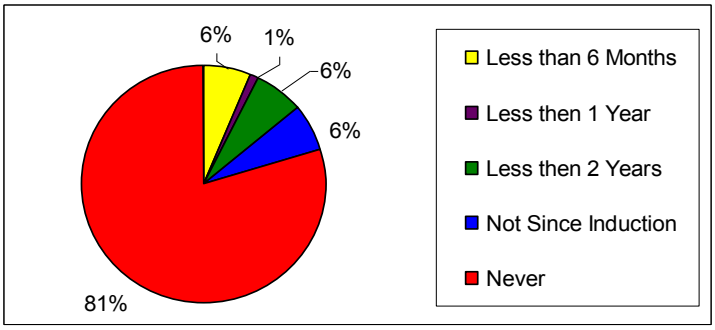


Figure 22. Time since last Data Protection Act training in Housing and Social Services

Both interviewed members of the Housing and Social Services management recommended practical training seminars as the most useful methods of education. They said repetitious reminders should follow the seminars. Both managers stressed the importance of these seminars being applicable and specific to the Housing and Social Services department. One manager reported that posters were effective reminders while the other said that they were seldom read. Employees were likewise asked for training suggestions in the surveys. Ten of 36 respondents proposed the use of seminars, while two said they would like to receive pamphlets. According to employee surveys about opinions of various training methods, pamphlets (with a 55% approval rate) and seminars (with a 54% approval rate) were the best-liked means of communication. As with the Chief Executive department, posters were least liked. Employee survey responses to different educational methods are shown in Figure 23.

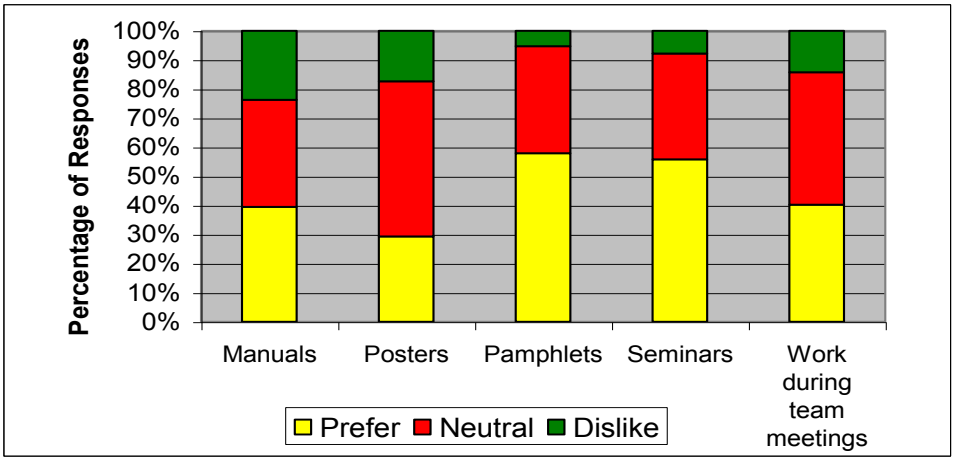


Figure 23. Housing and Social Services employees' opinions of various training methods

4.2.3 Finance

Our Finance department interviewee stated that all staff underwent data protection training before entry into the London Borough of Merton. This individual also said that there were seminars available for employees. Conversely, as Figure 24 illustrates, 46% of the surveyed employees of the Finance department said that they had never been trained in data protection. Another 21% had not had any training since their induction.

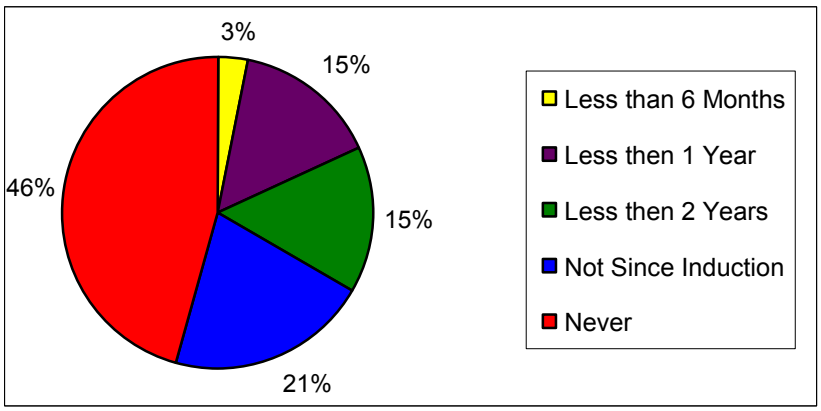


Figure 24. Time since last Data Protection Act training in the Finance department

The Finance department's manager cited team meetings as the most effective means of communication. In addition, this individual suggested specific training courses as a means of education, and stated that posters are seldom read. When surveyed employees were asked for any ideas concerning useful training methods, six of the twelve suggestions included a seminar or training course. There were five employees who proposed the use of a manual. Employees were then asked to state their feelings toward different training methods. As Figure 25 shows, 61% of respondents preferred seminars as an educational method, while the same amount preferred manuals.

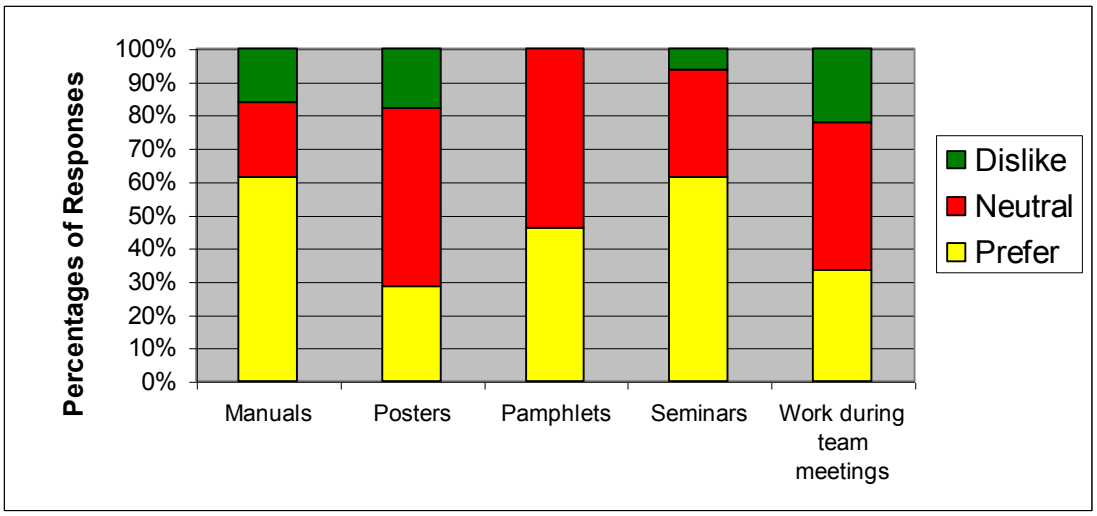


Figure 25. Finance department employees' opinions of various training methods

4.2.4 Environmental Services

The two individuals interviewed in the Environmental Services department stated that there was either no data protection training for employees, or none after induction into the London Borough of Merton. In support of this, when employees were asked how long it had been since their last data protection training, 74% replied that they had never been trained in this regard (Figure 26). However, 16% said that they had been through training within the last six months.

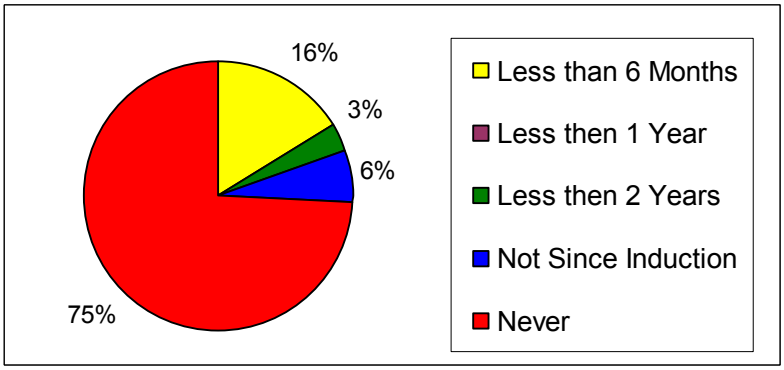


Figure 26. Time since last Data Protection Act training in Environmental Services

Both interviewees stated that specific interactive workshops were useful methods of education. In addition, one manager said that these should be followed up with written guidelines to which

employees could refer at any time. This individual suggested manuals in particular. When employees were surveyed about their feelings toward different training methods, seminars proved to be the best liked. As shown in Figure 27, 55% of respondents preferred this method, while only 3% disliked it. Manuals were the next best method received. They were preferred by 45% of the surveyed employees; however, 29% disliked this educational tool. In the survey, employees were further asked for their suggestions on Data Protection Act training. There were many diverse methods proposed, but there was one common factor. Seven of the seventeen respondents stressed that training should be specific to their needs.

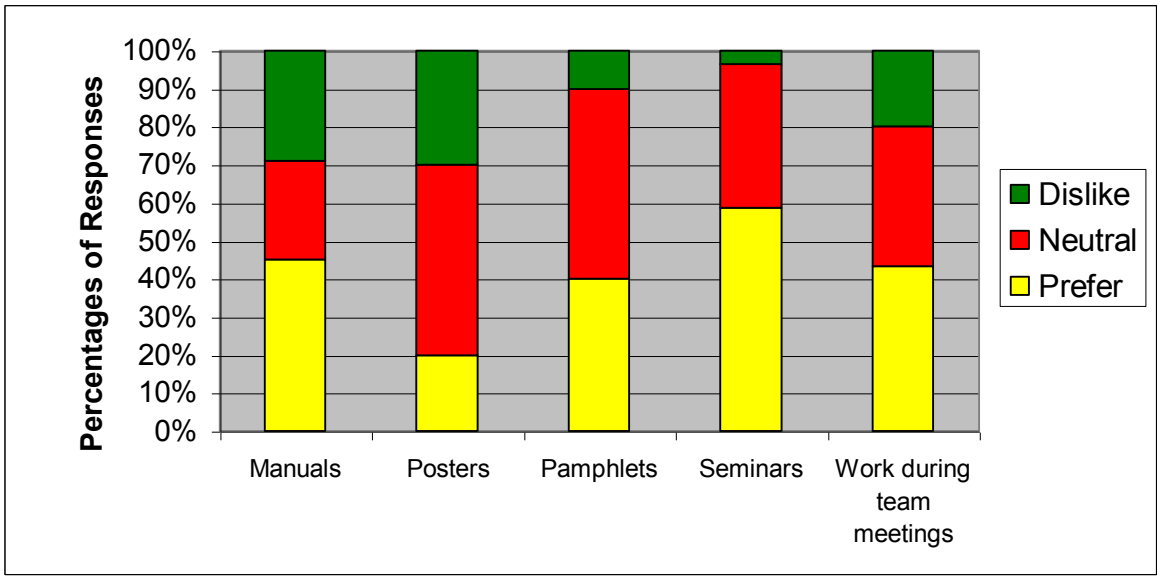


Figure 27. Environmental Services employees' opinions of various training methods

4.2.5 Education, Leisure and Libraries

We asked the interviewee from Education, Leisure and Libraries about data protection education subordinates in this department. This individual stated that there was currently none provided. We then surveyed employees asked when their last training on the Data Protection Act occurred. As Figure 28

illustrates, 94% said they had never received data protection training. There were no employees that had been through data protection training in the past year.

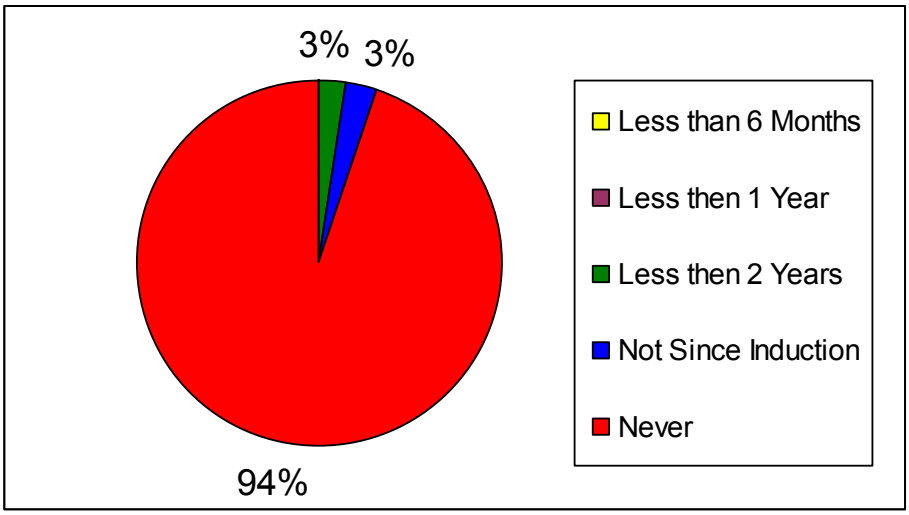


Figure 28. Time since last Data Protection Act training in Education, Leisure and Libraries

Given the current lack of training experienced in the Education, Leisure and Libraries department, the manager we interviewed stated that training should be broad to begin with. This individual additionally suggested that a series of presentations take place during the course of the day. These presentations would outline the basics of the Data Protection Act of 1998. Their varying times would allow all employees to attend. However, when employees were surveyed for data protection training suggestions, three of nine respondents said that the training should be specific to their occupation. Four of the responses included a training seminar. Two respondents suggested that data protection education take place during team meetings. The surveyed employees were then asked to rate their feelings toward various methods of education. As is shown in Figure 29, work during team meetings was the most favoured. Fifty-four percent of surveyed employees preferred this method of training. Pamphlets had a 36% approval rate, while the least amount of respondents disliked pamphlets.

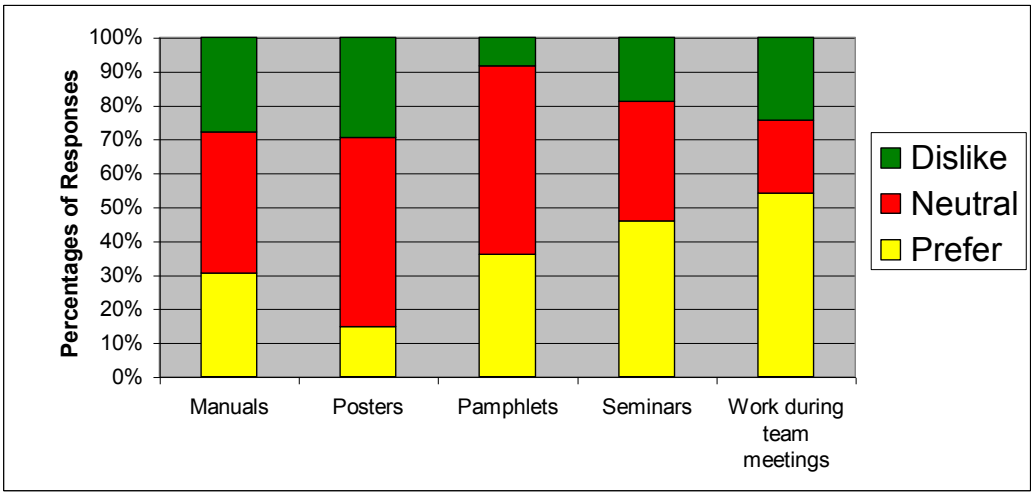


Figure 29. Education, Leisure and Libraries employees' opinions of various training methods

4.2.6 Common Results

Managers mentioned a lack of data protection training. Of the eight managers interviewed, five managers reported that their departments had no training beyond an individual's induction when he or she first came to the London Borough of Merton. Two of the interviewees, from separate departments, indicated that there was no data protection training in their department whatsoever. When asked when was the last time they had been trained in data protection, 74% of the surveyed employees replied "never." Figure 30 shows that of the remaining employees, 6% have had training within the past two years and 3% within the past year.

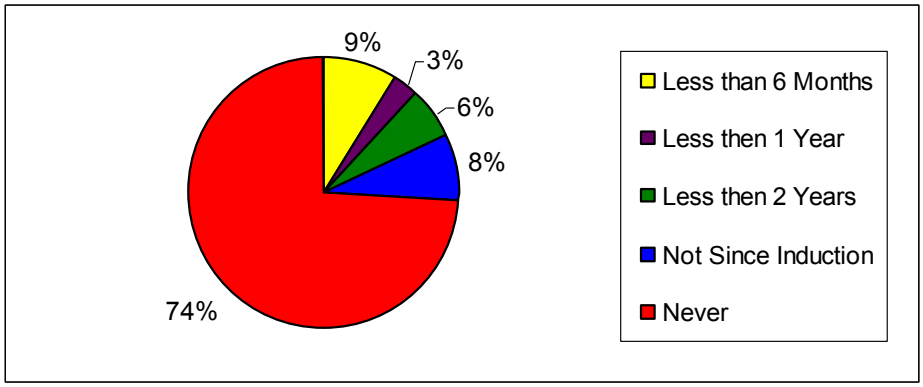


Figure 30. Time since last Data Protection Act training in the entire Civic Centre

Most managers cited team meetings as the most effective means of communication. The most suggested training form was seminars. To compare managers' perceptions to employees' opinions, we asked surveyed individuals to state their feelings about different training methods. As Figure 31 shows, seminars were the method best received by employees in the Civic Centre, having the highest percentage of respondents preferring them. However, contrary to managers' beliefs, work during team meetings had rates of approval below that of pamphlets and seminars. Pamphlets were the most liked method of reminders. Half of the respondents classified them as preferred, and they had the fewest number of respondents disliking them. Posters were generally neutrally received.

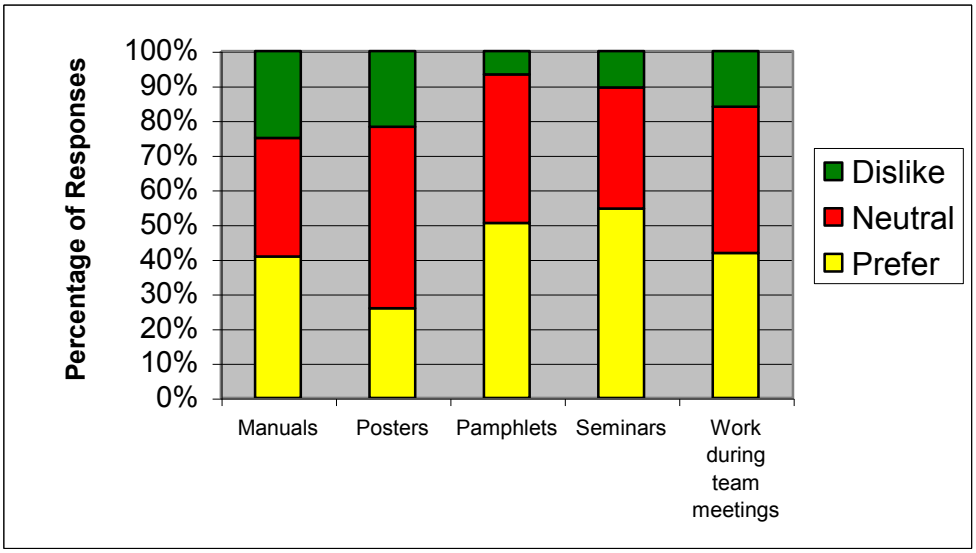


Figure 31. The all Civic Centre employees' Opinions of various training methods

Chapter 5 – Conclusions and Recommendations

We analysed specific areas concerning Data Protection Act awareness and training methods from five departments. Following this, we developed a set of recommendations detailing the needs of each department. First, we concluded which areas will be the focal points of each educational plan. Second, we determined how each plan would be best delivered. Although training plans developed based on these recommendations would be effective, there are several areas of research that we feel would facilitate the creation of better plans.

5.1 General Civic Centre Training Plan

Given the trends found in all five departments, we determined that it would be best to include a section of the training plan that would be universal for the entire Civic Centre staff. In addition, a publicity plan should be implemented. This will keep Data Protection Act compliance in the forefront of employees' minds.

5.1.1 Civic Centre Training Topics

There were several aspects that need to be included in the general London Borough of Merton Data Protection Act compliance training plan. The information content covered in this section of the training plan would be the same for all departments, though the method of delivery would vary. This will consist of basic principles and fundamental facts that will be conveyed to each department through the means deemed most useful for that department. First, each training plan should begin with a basic overview of the Data Protection Act. This would ensure that all trainees understand the basis of their training, even those that have never had any data protection education before. Next, all five plans should include information about the regulations regarding data subject requests. In order for this to be

done, the London Borough of Merton should develop a comprehensive written procedure for handling these requests. Every department should have a copy of this procedure.

The second topic that should be covered in the generalised training plan is interdepartmental security. Employees must be informed that they may not transfer information freely to other Civic Centre employees. Employees should be informed of what information may and may not be released to which employees.

5.1.2 Publicity Plan

There are two main methods that we recommend for publicising data protection awareness: posters and payslip attachments. Although there was a low percentage of employees that listed posters as a preferred method of training, the response was not largely negative either. Most respondents stated a neutral stance toward posters. In addition, posters will not be a stand-alone method of training. We recommend that posters be placed in lifts as most passengers in lifts tend to avoid eye contact, leaving them looking at the lift walls. These posters need to be eye-catching and make a connection with the readers on a personal level. Several examples of possible posters to be used are included in Appendix O.

Employees were not surveyed concerning their opinions about payslip attachments. However, this idea was suggested by several managers as well as one survey respondent. When London Borough of Merton employees receive their payslips, often a reminder or memo is attached. The data protection publicity attachments will carry a short message to the employee about an aspect of the Data Protection Act. These aspects will range from the effects of non-compliance to reminders about particular regulations. Appendix P contains a listing of possible memos that could be attached.

5.2 Departmental Training Plan Details

Although there were subjects that must be universally covered, there are other areas of data protection that should receive different focus in different departments. Results of departmental interviews and surveys showed that each of the five departments had particular areas that were in urgent need of data protection training. The needs for each plan were determined by the application of the Data Protection Act of 1998 to each department. Training should be designed to focus on the aspects of the act that are most misunderstood. Each department responded positively to different methods of training, thus training must be delivered to each department in diverse ways.

5.2.1 Chief Executive

There is only one main data protection issue that needs to be addressed in the Chief Executive department in addition to the matters that concern the entire London Borough of Merton. This is primarily that employees must be informed about issues of data security. There is a substantial section of the Chief Executive branch that feels that it is acceptable to keep personal databases on members of the public. This practice, however, compromises security as well as the ability of the department to track information.

Data Protection Act training for this department should mostly take place in team meetings, as this was the method of in-depth training that received the highest approval rate in the department. This method should be used to present the majority of factual information. During or following these meetings, employees should be given pamphlets that reinforce the information presented in the meetings. These pamphlets should list facts or frequently asked questions and could be used as a quick reference guide.

5.2.2 Housing and Social Services

There are three specific subjects that need to be addressed in the Housing and Social Services department. First, employees should be informed of what information to give out in different circumstances. A significant fraction of employees in this department were unaware of what information may or may not be released in circumstances with sensitive information. Second, all individuals need to be informed of the proper manners for file handling. Employees said that this was the greatest cause of inaccurate personal data. It is possible that employees are already aware of the correct file handling techniques and simply need to be reminded of the importance of this form of data protection. In addition to this, files must be reviewed for inaccurate information. It was suggested that a file updating policy be implemented. Therefore, we recommend that protocol be created. An overview of this procedure can be included in the Housing and Social Services training plan.

In this department, seminars have been shown to be the best form of in-depth communication. Consequently, we recommend that the base factual instruction be presented to employees in this form. It was mentioned repeatedly that seminars must be specific and applicable to Housing and Social Services. It was also said that interactive seminars would be more effective than lectures. Managers of this department stated that data protection guidelines must be repeatedly mentioned to employees. We recommend that pamphlets be distributed on a regular basis to aid employees memories. Each should detail a specific area of training. In addition to this, short reminders should be given at staff meetings.

5.2.3 Finance

The Finance department was not shown to have any data protection awareness issues that were not common to the entire London Borough of Merton. However, they did describe themselves as lacking in-depth knowledge of the Data Protection Act. Therefore, at this time we suggest that only the information included in the basic training plan be presented in the Finance department. This

information should be presented in seminars, as these are the most well received training method. The management of the Finance department stated that manuals were an effective means of education, and that employees responded well to this tool. This was reinforced by our surveys, in which individuals rated manuals among the most preferred manners of training. However, given the lack of specific problems revealed in the Finance department, manuals do not appear to be a needed measure.

5.2.4 Environmental Services

There were two main data protection issues that came to light through the interviews and surveys we conducted in Environmental Services. First, there is the matter of interdepartmental security. Since this department receives most of its files from other departments, it does not keep many official files. There is a large amount of data transfer both into and out of Environmental Services as well. Employees are confused about the details of personal data files that may or may not be released to other departments. The second concern is data security. Given that half of the Environmental Services employees are not aware how to password protect a file, and about a third of their files remain on their desks indefinitely, it is important that the educational plan include regulations on file security. It would be helpful if employees were taught how to password protect files. In addition, they should be informed about the proper manner in which to store information.

Seminars should be the main method of training in Environmental Services. After the aforementioned details are covered in these seminars, employees should be given a manual. These manuals will remind individuals about how to correctly store information both in electronic and paper form. In addition, it should give a list of specific information that may be released to different employees. These manuals need to be concise, and written in every-day English.

5.2.5 Education, Leisure and Libraries

There is an extremely high percentage (94%) of people in Education, Leisure and Libraries that have never received data protection training. Thus, it will probably be necessary to spend more time on the basics of the Data Protection Act of 1998 here than in other departments. This would include an explanation of the eight principles of data protection as well as the legal consequences of non-compliance with the act.

As in two other departments, an issue that needs to be addressed in Education, Leisure and Libraries is what information may be given in different circumstances. Employees of this department should be trained in what information should be given when an individual requests information about a third party.

Education, Leisure and Libraries employees indicated that they prefer team-meetings above other means of in-depth training. Accordingly, we recommend that this educational tool be used to communicate the basics of data protection as well as provide an in-depth discussion of what information may be released when members of the public request data. It would also be helpful if employees could ask questions about specific scenarios. These team-meetings should be followed up with pamphlets that remind employees of the basics within the Data Protection Act. In addition, these pamphlets should provide a written account of how to deal with various types of data subject requests. An example of a pamphlet to be used in the Education, Leisure, and Libraries can be found in Appendix Q.

5.3 Recommendations for Further Research

There were several areas of research that were not explored in this project that would be beneficial to the London Borough of Merton in the development of a comprehensive data protection training

program. One of these aspects is the issue of untrained operative staff. Another is the relationship of the Caldicott guidelines and the Data Protection Act. Lastly, since the Borough is organised by a tiered system, it would be helpful to examine the difference between managerial and non-managerial data protection awareness. This would also help to evaluate the effectiveness of the trickle-down method of communication.

Operative staff can be defined as those that are on the front lines of data protection. These employees do not have much contact with the Civic Centre. However, they are London Borough of Merton employees and they do have access to personal data. These employees include social workers, transportation staff and teachers. They maintain many temporary files, and the degree of security of these files is unknown. In order for the London Borough of Merton to fully comply with Data Protection Act regulations, it is important to know the operative staff's level of awareness. Following, an educational plan must be developed to meet the needs of these employees. We did not have the time or the resources to evaluate operative staff in the course of our seven-week project. However, given the importance of these employees' Data Protection Act compliance, we suggest that research be done into the data protection needs of the operative staff.

The Housing and Social Services department is implementing the Caldicott standards. Although these guidelines are not legally binding, most employees in this department follow the Caldicott standards as their principal means of data protection. Given the legal predominance of the Data Protection Act of 1998, it is imperative that Housing and Social Services employees comply with it. Therefore, research needs to be performed to ensure that all Caldicott standards conform to Data Protection Act regulations. If Caldicott standards do not comply completely, the training program for the Housing and

Social Services department must be designed to ensure that employees are aware of the areas in which Caldicott standards are not sufficient.

The last area requiring further research is the possible disparity between managers' and subordinates' knowledge of the Data Protection Act of 1998. When survey results were analysed, they were classified according to the respondent's department. This provided a basis for recommendations for departmentally specific training plans. However, there is a possibility that managers and subordinates would benefit most from different training due to differing knowledge. Therefore, it would be helpful for the London Borough of Merton to conduct a study comparing data protection awareness of managerial and non-managerial staff.

5.4 Implications

We have provided the London Borough of Merton with a set of recommendations for departmental data protection training plans. With these recommendations, they are now able to begin the systematic development of educational plans that cover the needs of the entire Borough as well as target the needs of the specific departments. As our liaison stated, "For the first time this council will have a structured approach to implementing the Data Protection Act and raising awareness with employees" (Guild, 2003). Once these training plans are developed and implemented, we hope they will raise employee compliance with the Data Protection Act, thus better protecting the people of Merton.

Bibliography

Ackroyd, S.; and Hughes, J. (1992). Data Collection in Context. Malaysia: PMS.

Adair, J. (1973). Training for Communication. Guilford, Surrey: Biddles Limited.

Ayoade, J. O.; and Kosuge, T. (2002). Breakthrough in privacy concerns and lawful access conflicts, Telematics and Informatics, Vol. 19, n. 4. p. 273-289.

Berg, B. L. (2001). Qualitative Research Methods for Social Sciences. Allyn and Bacon, Boston.

Bergin, F. J. (1990). Practical Communication. Singapore: Pitman Publishing.

Boehmer, R. G., and Palmer, T S. (1993). The 1992 EC Data Protection Proposal: An Examination of Its Implications for U.S. Business and U.S. Privacy Law. American Business Law Journal 31 Sept 1993.

Branscomb, A. (1995). Who Owns Information?: From Privacy to Public Access. Basic Books. New York, New York.

Burke, E. (2003). London Borough of Merton: Human Resources Manager. Personal Interview, 22nd January 2002.

Bushkin, A., and Schaen S. (1976) The Privacy Act of 1974: A Reference Manual for Compliance. System Development Corporation. McLean , Virginia.

Carey, Peter (1998) Blackstone's Guide to the Data Protection Act of 1998 London: Blackstone Press Ltd.

Carey, P., and Russell, C. (2000). Data Protection in the UK. London: Blackstone Press Ltd.

Cate, F. H. (1997). Privacy in the Information Age. Washington D.C.: Brookings Institution Press.

Consumer Privacy Guide.org: Center for Democracy and Technology (2001) Retrieved December 9th, 2002, from the World Wide Web: http://www.consumerprivacyguide.org

Craig, L. (1976). Training and Development Handbook. McGraw-Hill: New York, New York.

Dagsputa, S., Hettigae, H., and Wheeler, D. (2000). What improves environmental compliance? Evidence from Mexican industry, Journal of Environmental Economics and Management. vol. 39, p. 39-66.

Data Protection Act of 1998 (1998). *The United Kingdom,* Chapter 29.

De Vaus, D. A. (1991). Surveys in Social Research. Third Edition. Guilford: Biddles, Ltd.

Donaldson, A. (2000). Policy for cryptography in healthcare — a view from the NHS, International Journal of Medical Informatics, Vol. 60, n. 2, p. 105-110.

EU Directive (1994). Directive *94/ 46 /EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal data and on the Free Movement of Such Data* The European Parliament and the Council of the European Union.

Furnham, A. (1998). The Psychology of Managerial Incompetence: A Sceptic's Dictionary of Modern Organizational Issues. UK: Athenaeum Press Ltd.

Gómez-Mejía, L. R., Balkin, D. B., and Cardy, R. L. (2001). Managing Human Resources Prentice-Hall Inc.: Upper Saddle River, NJ.

Gozna, L. F., Vrij, A., and Bull, R. (2001). The impact of individual differences on perceptions of lying in everyday life and in a high stake situation, Personality and Individual Differences, Vol. 31, no. 7, p. 1203-1216.

Guild, S. (2003). Civic Centre: Data Protection Officer. Personal Interview, January 14th 2003.

Hakkinen, K. (1995). A learning-by-doing strategy to improve top management involvement in safety, Safety Science, Vol. 20, p. 299-304.

Henderson, H. (1999). Privacy in the Information Age. New York: Facts on File Inc.

Jay, R., and Hamilton, A. (1999). Data Protection: Law and Practice. London: Sweet and Maxwell Ltd.

Karina, A. (1998). Handbooks as a tool for organisational learning: a case study. Journal of Engineering and Technology Management, Volume 15, Issues 2-3, Pages 201-228.

Keats D. (2001). Interview: A Practical Guide for Students and Professionals Buckingham, Open University Press.

Kennedy, C., and Alderman E. (1995). The Right to Privacy. Vancouver, WA. Vintage Books.

Loughary, J. (1979). Producing Workshops, Seminars, and Short Courses: A Trainer's Handbook. Cambridge Book Co.

Reidenberg, J. R. (1992). Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? Federal Communications Law Journal Vol.44.

Simpson, W. A. (1989). Motivation: Notes for Managers. Northampton: Belmont Press.

Stokols, D., McMahan, S., and Clitheroe, H. C. Jr., and Wells, M. (2001). Enhancing corporate compliance with worksite safety and health legislation. Journal of Safety Research. Vol. 32, p. 441-463.

Torbjorn, R., Hale, A. R. (1995). Managers' attitudes toward safety and accident prevention, Safety Science, Vol. p. 1-16.

Wilson, Brent G. (1997, March). Reflections on constructivism and instructional design. *Instructional Development Paradigms, 18 pages.*

Wright, M. A. (1998). The Need for Information Security Education, Computer Fraud & Security, Vol. 1998, n. 8, p. 14-17

Appendix A: Organisation of the London Borough of Merton

(Source: http://www.dataprotection.gov.uk/commissioner.htm)

The borough of Merton is based around 5 key priorities for 2002 -2003:

1) EDUCATION MERTON - the achievement of standards of excellence in our schools and colleges and inclusive access to learning, the arts and sport.
2) CARING MERTON - support for vulnerable children that equals the standards of the best and support for vulnerable adults that meets their needs while maximising their independence
3) SAFE, CLEAN AND GREEN MERTON - a safe and clean environment in our streets and open spaces to improve sustainability and provide a high quality of life for residents.
4) A THRIVING MERTON - regeneration of town centres and neighbourhoods to provide an attractive environment in which to live, visit and work.
5) EQUALITIES MERTON - full and equal access to learning, employment, services and cultural life and the celebration of diversity.

There are 7 heads of service in the Merton Borough Council:

1) Diane Bailey: Scrutiny and Policy
2) Gurmel Bansal: Information Technology Services
3) Julie Belvir: Legal Services and Local Land Charges
4) Michael Bentley: Electoral Services
5) Valerie Jones: Human Resources
6) Rob Moran: Partnerships
7) Gene Saunders: Communications and Democratic Services

The Council itself is composed of 60 councillors, with a staff of 5,500 council officers and teachers.

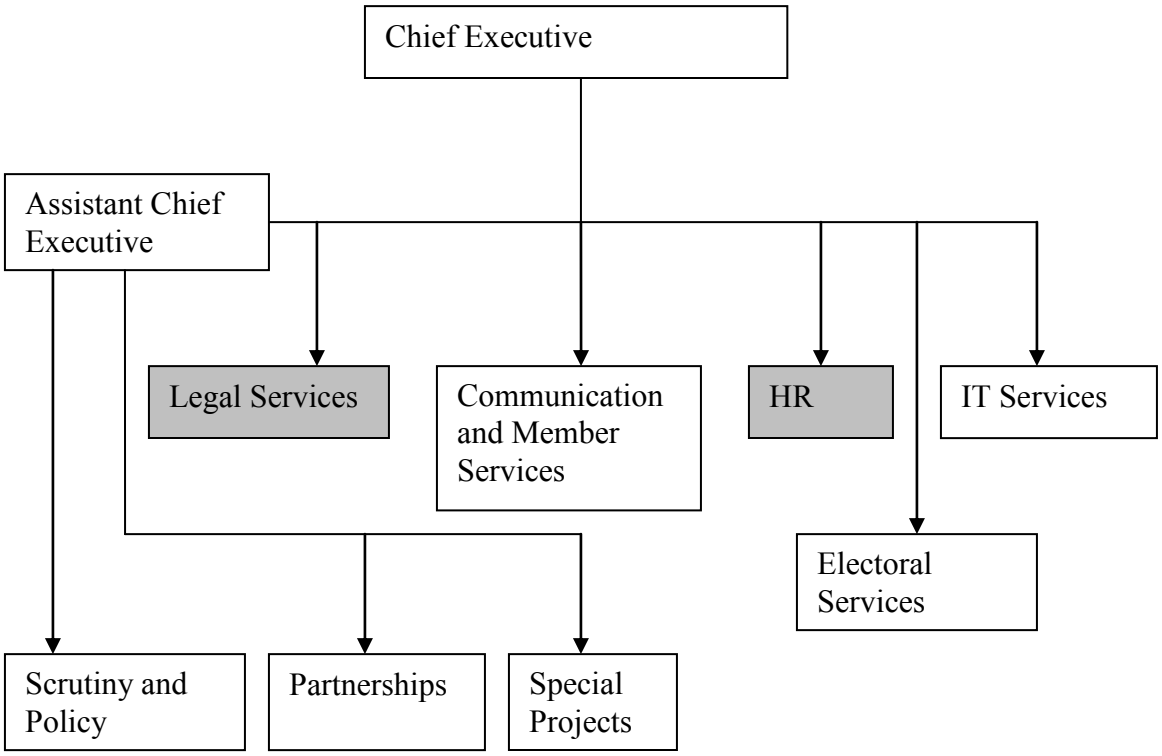
The Information Commissioner in the UK is Mr. Richard Thomas. He enforces and oversees the Data Protection Act of 1998 as well as the Freedom of Information Act of 2000. As information commissioner, he has the following mission statement:

> "We shall develop respect for the private lives of individuals and encourage the openness and accountability of public authorities.
>
> -by promoting good information handling practice and enforcing data protection and freedom of information legislation; and
>
> -by seeking to influence national and international thinking on privacy and information access issues."

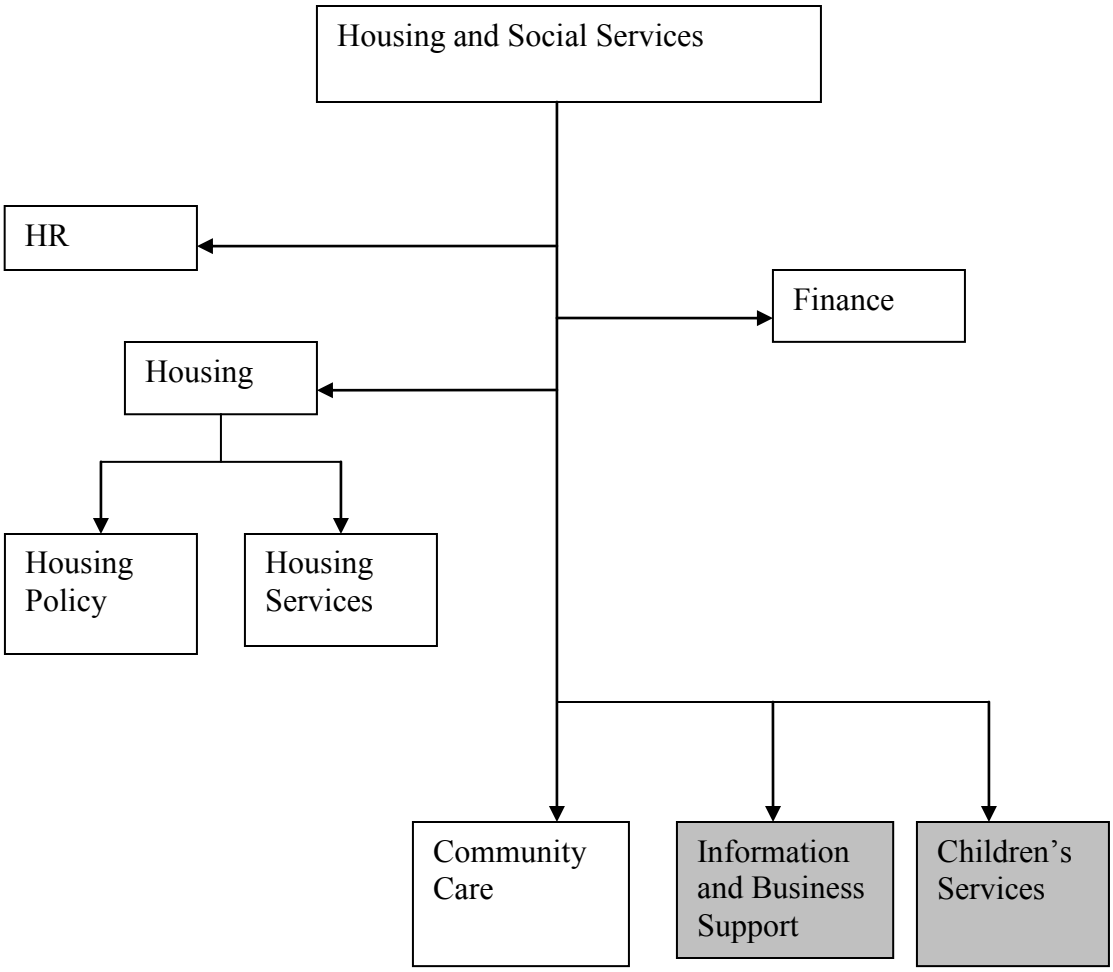
Flowchart of London Borough of Merton Organisational Structure by Department

Gray boxes denote divisions in which we interviewed managers.

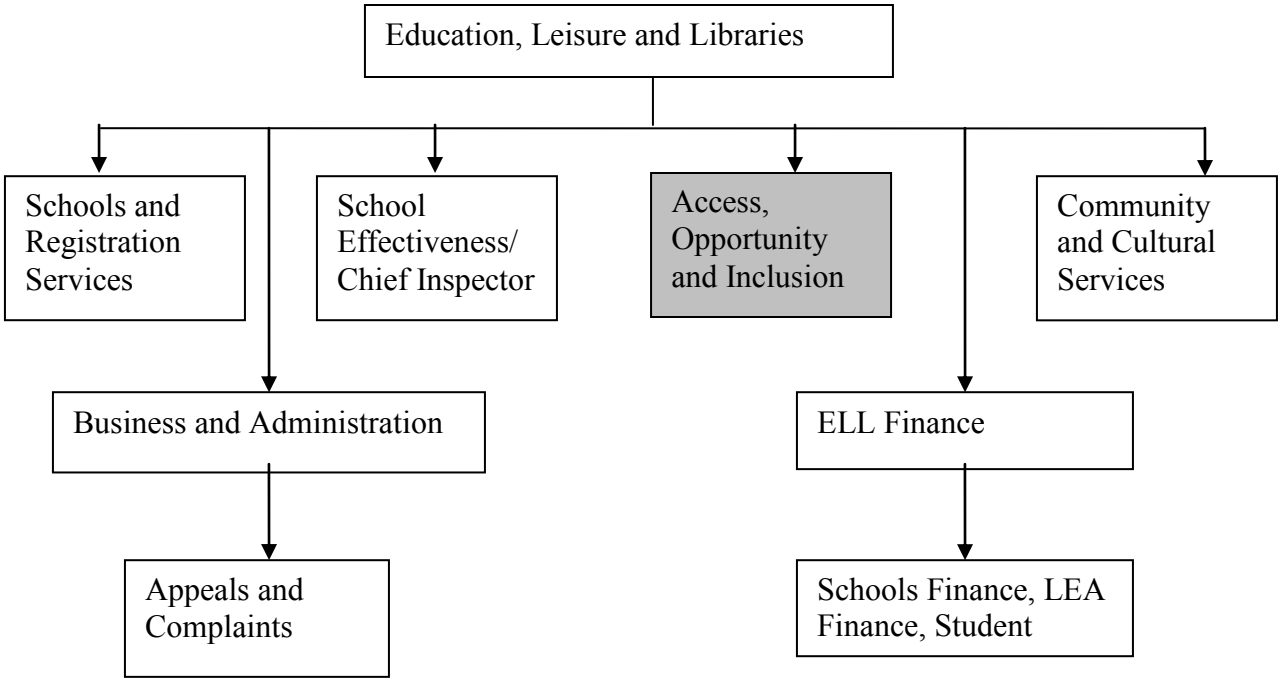
Chief Executive



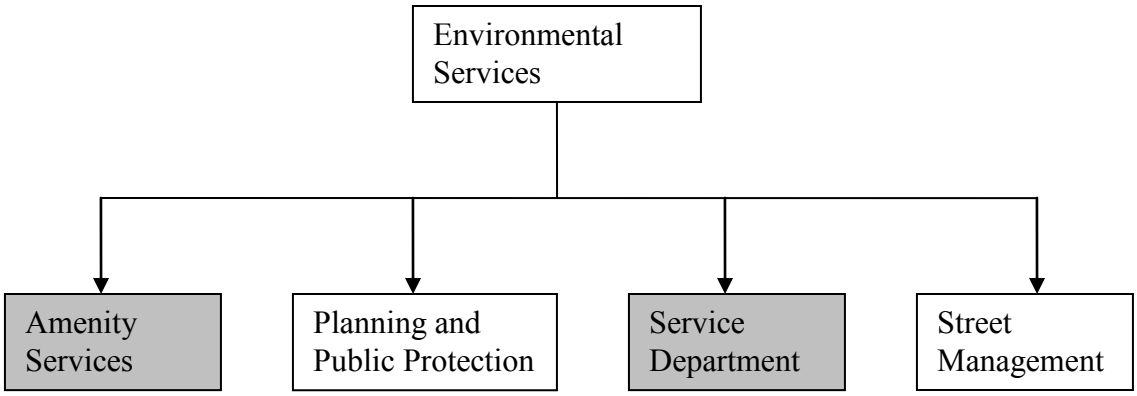
Housing and Social Services



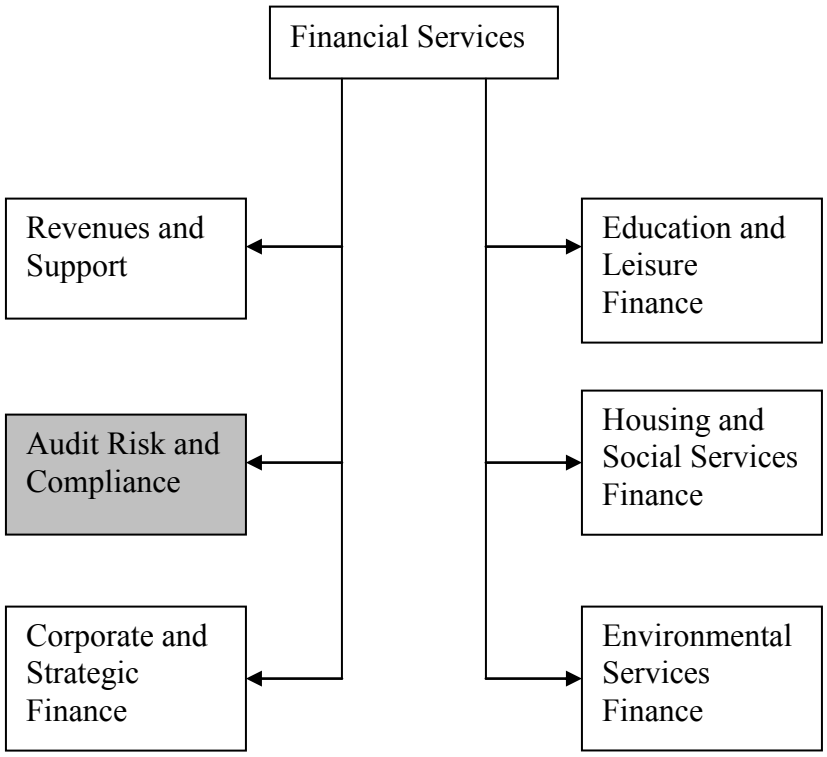
Education, Leisure and Libraries



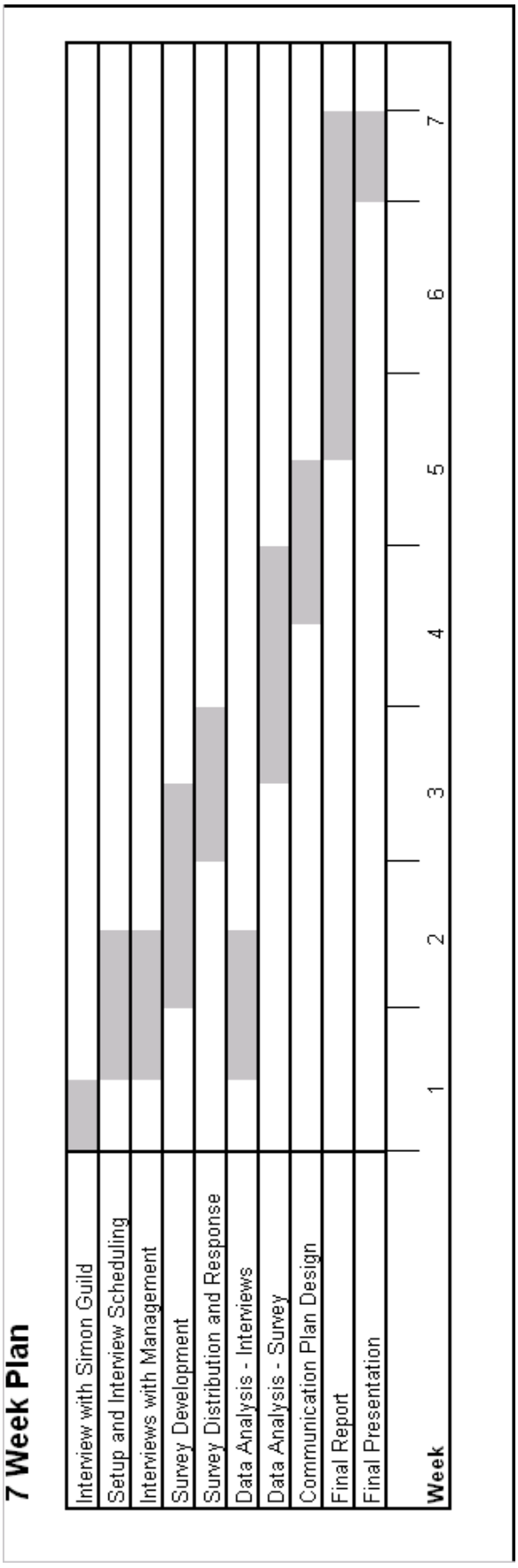
Environmental Services



Finance


Financial Services
Revenues and Support
Audit Risk and Compliance
Corporate and Strategic Finance
Education and Leisure Finance
Housing and Social Services Finance
Environmental Services Finance

Appendix B: Project Timeline



Appendix C: Interview Guide (Simon Guild)

Scope: Do you want an educational plan or do we want to alter the process of data subject requests?

I. Background
- A. Are there any areas that you see are lacking information and should be amended?
- B. Are there any sources you would suggest investigating?

II. Review of Planned Methodology
- A. General: Are there any other strategies that you believe may be helpful?
- B. Interviews with management
  1. Who should we interview? (How many people should be interviewed?)
  2. When will the interviews be?
  3. Are there any specific questions we should include in our interviews?
- C. Surveys of general employees
  1. Whom do you suggest we send the surveys to? (Only departments who were interviewed?)
  3. Are there any specific questions we should include in our survey?
  4. What do you think of the idea of an incentive of some sort for survey response? Any suggestions for an incentive?
- D. Analysis of data
  1. Are there specific factors we should focus on upon conducting analysis?
  2. What are the questions you would like answered from our analysis?

III. Education Plan
- A. What are the present education plans which are in effect?
- B. What are your expectations for a new educational plan, if at all you expect one?

Appendix D: Interview Guide for Department Management

We are a group of students from WPI who are here to do a project on the uses and efficiency of the DPA at the London Borough of Merton. The purpose of our project is to make recommendations to the DP officer for a straight-forward, useful guide that would help you know what your responsibilities are with respect to DPA 98. We are talking to you to get a feel for what is going on within your department and to get your perceptions about what the people around you think about DPA compliance. Do not worry about giving the "right" answer. We are just looking for your perceptions and observations. We have a form here we would like you to sign that explains how the interview will be used.

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?
What is the main effect (if any) of the DPA 98 on your department? How has the new law changed the way that things work? Changes in efficiency, office attitude, security…
Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…
What are the greatest obstacles to compliance In your department?

II) What training do the employees in your department currently have in DP?
What methods are currently used for education and training within your department?
Which of these methods are the most useful, which would you recommend for DPA education?

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?

II) How do you protect individuals' data?
Are you letting employees and clients know about this?

III) What are the regulations on security? Access, taking information home.

IV) Are you aware what will happen if someone wants to see the info held on them? Process and documentation

V) What means do you currently have to keep data up-to-date?
Do you have any policy for prevent the excessive retention of data?

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?

SENSITIVE DATA

Sensitive data: racial origin, ethnicity, politics, beliefs, health, sexual preferences, criminal charges and convictions.

I) Do you take special precautions with sensitive data that you possess? What are they?

Appendix E: Interview Consent Form

This interview will be recorded on tape. The recording is to be used for analysis purposes only. This tape will not be heard by anyone other than the WPI students in the Data Protection Act Compliance project group. Neither your identity nor responses will be passed on to your superiors. Your responses will have no effect on your professional standing.

I have read this information and understand consent to the aforementioned terms.

_____ _____/_____/_____

Printed name Date

_____

Signature

Appendix F: Interview Transcripts

The transcripts of the managerial interviews conducted are as follows. The interviewees were guaranteed anonymity, thus any identifying information has been deleted from the transcripts. The transcripts are also in the form of notes, as taken during the interviews, thus not all responses are completely reflected by that provided below. Some questions may remain blank as either nothing useful was noted in response or the response contained identifying information.

Interview #1

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?
Something about personal records for some services. Computerised systems for holding files, support to other depts. when they ask for files.

What is the main effect (if any) of the DPA 98 on your department? How has the new law changed the way that things work? Changes in efficiency, office attitude, security…
Raised general awareness. People are more aware that they need to be careful with information. Lack understanding of the specifics as they apply.

Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…
What are the greatest obstacles to compliance In your department?
They don't have specifics. Insufficient clarity for individuals, and of info. Legal jargon. Not systems across the depts. Trickle down is not effective.

II) What training do the employees in your department currently have in DP?

What methods are currently used for education and training within your department?

Which of these methods are the most useful, which would you recommend for DPA education?
Two levels: one—resources for employees, written notes, handbooks, guides to refer to. Two—training specifics to individuals, no blanket training, practical.

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…
Team meetings, not e-mail. Third and 4th tier were most useful for training, trickle down doesn't always work, operatives don't always get info.

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?

Sensitive data—yes, non-sensitive, control of destination DNE. Unrestricted access to info, no controls for interdepartmental transfer.

II) How do you protect individuals' data?

Are you letting employees and clients know about this?

III) What are the regulations on security? Access, taking information home

----

IV) Are you aware what happens if someone wants to see the info held on them? Process and documentation

If someone comes in to ask for info they would get it. If there was a request, there is no documented way of dealing with it. Timeliness is a problem, multiple files. Depends on type and amt of info, don't hold a lot of info. "Everybody hold the records they need to."

V) What means do you currently have to keep data up-to-date?
Do you have any policy for prevent the excessive retention of data?

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?

Interview #2

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?
Spec. principles

What is the main effect (if any) of the DPA 98 on your department?
Prior: info such as credit status could be gotten through commercial routes could go "fishing" for info about fraud
Now: requires due cause, evidence to obtain information about anyone

How has the new law changed the way that things work? Changes in efficiency, office attitude, security…
See above.

Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…
Yes, can get in trouble, evidence can be dismissed, cases thrown out,

What are the greatest obstacles to compliance in your department?

II) What training do the employees in your department currently have in DP?
Everyone trained in DPA before entry, seminars

What methods are currently used for education and training within your department?
Manual for everybody—coaching for grade B. No resentment, grow out of its use, manual updated.
Training for spec. issues

Which of these methods are the most useful, which would you recommend for DPA education?
Posters/ Bulletin boards are bad, no one reads them. Spec. training courses is good. Global e-mails sometimes work.

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…
Heads of service meeting, 0.5-1.0 days, info dispersed through team meetings.

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?
Yes, forms are scanned in. They're tracked on the computer by a numerical code. If not tracked, people don't get money, or the department doesn't get the $. Desktop imaging for tracking.

II) How do you protect individuals' data?

Are you letting employees and clients know about this?

Clause on the form, knowledge of purpose, what info, but not mode of transport or storage.

III) What are the regulations on security? Access, taking information home

---

IV) Are you aware what will happen if someone wants to see the info held on them? Process and documentation

No procedure, informal exchange of information if someone came in and asked for their data. No one as of yet has made a request. No info given out. If simple request: probably fulfilled in 40 days, not if all-encompassing. Employees are aware of the possibility of requests.

V) What means do you currently have to keep data up-to-date?

Individual's legal obligation to keep borough up-to-date. Renewal of data every 6 mo. required for continued service. Penalties for lack of updates by individ.

Do you have any policy to prevent the excessive retention of data?

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?

What people know about DP? Extent of knowledge. Awareness of need to meet provisions.

<u>SENSITIVE DATA</u>

II) Here are some examples of sensitive data: racial origin, ethnicity, politics, beliefs, health, sexual preferences, criminal charges and convictions.

III) Do you take special precautions with sensitive data that you possess? What are they?

EVERYTHING is sensitive data.

Interview #3

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?

What is the main effect (if any) of the DPA 98 on your department? How has the new law changed the way that things work? Changes in efficiency, office attitude, security…

No Changes – there has a change within the department less than 18 months – staff is new to problem..

Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…

What are the greatest obstacles to compliance In your department?

Employees are aware of it but not aware of how to apply the DPA98 to problems. General terms comply – but not intentionally

II) What training do the employees in your department currently have in DP?

No

What methods are currently used for education and training within your department?

Corporate training – invited Simon Guild

Which of these methods are the most useful, which would you recommend for DPA education?

Team meetings – smaller groups, open forms, notes on lifts, notice boards, Reminders

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…

Team meetings

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?

There is no way to track information. There are a lot of managers that keep information about their staff and I don't know where they are held and I have a concern with it.

II) How do you protect individuals' data?

Files – locked in key

Are you letting employees and clients know about this?

III) What are the regulations on security? Access, taking information home

They are all locked in files but anyone may go in. We take care of it but there is no actual policy.

IV) Are you aware what happens if someone wants to see the info held on them? Process and documentation

No link within department ----- – I think 24 hrs…(she wasn't sure like???) no control because any manager may randomly come in.

V) What means do you currently have to keep data up-to-date?
Do you have any policy for prevent the excessive retention of data?

They are out of date because there are too many files and no process of review.

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

Team meetings and Reminders

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?

She asked for time so she could Email us with any relevant question

Interview #4

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?
Dictates requirements for sharing information, length and contents of records.

What is the main effect (if any) of the DPA 98 on your department? How has the new law changed the way that things work? Changes in efficiency, office attitude, security…
How they keep records, amount kept, making sure that it is necessary and that only necessary information is kept. People feel that they have legal backing for refusing to give information.

Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…
Yes, as far as [certain workers] were knowledgeable and compliant about security. Files may be excessive and opinionated. Concerned with interdepartmental sharing of information (personnel illness). Worried about file security—files on disk, should be on hard drive and pass-word protected. People may talk about cases within the Borough itself.

What are the greatest obstacles to compliance in your department?
Unclear movement of data. Lack of knowledge of process, don't think about the DPA. Not sure of interdepartmental security levels.

II) What training do the employees in your department currently have in DP?
Have had training in school for DP, have training seminars every 6 weeks, may be on DP. Have long been subject to DP legislation, mostly under Caldicott. Trained in info gathering and recording.

What methods are currently used for education and training within your department?
Training days every 6 weeks, monthly staff meetings, initial induction.

Which of these methods are the most useful, which would you recommend for DPA education?
Most successful=briefings, repetition, 5 times. Re-tell when return, remind by e-mail

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…
Staff meetings=best, team managers should trickle down, Intranet policies, if confusing, use seminars. Seminars should be interactive.

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?
Good tracking, a new system with Caldicott.

II) How do you protect individuals' data?

Files are locked, each s.w. is responsible for case security.

Are you letting employees and clients know about this?
Consent forms were signed, when info was given, the purposes were stated.

III) What are the regulations on security? Access, taking information home
---

IV) Are you aware what will happen if someone wants to see the info held on them? Process and documentation
Not new for [specific department]., info requests since '84, but before they only had to provide a summary, now give individ the info they want, not too much. 5-6 formal requests/yr. with 1 or 2 small requests/week. Policy in place for handling all requests, although they're not always handled on time. Sort through info: legal advice is exempt. Turn around time dependent on amt. (don't want to give info that might be lost—incriminate someone.) Most people already have the info that [department] has.

IV) What means do you currently have to keep data up-to-date?
Need to go through files and check that they are up-to-date.

Do you have any policy for prevent the excessive retention of data?
Problematic, a lot of old info needed to be sorted through. Biggest change, biggest problem.

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?
Awareness to confidentiality? How do they feel about DPA? Routine security consciousness? Computerized system security?

Interview #5

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?

. 2 locations of files, civic centre and depot. What info is kept where? Clients: Evaluation process for contractors: what is known, what not?

What is the main effect (if any) of the DPA 98 on your department? How has the new law changed the way that things work? Changes in efficiency, office attitude, security…

Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…

What are the greatest obstacles to compliance In your department?

Office staff: Is careful about maintaining records, don't understand specifics and application. Not concerned, not bothered. Too much else to do. No personal effect, no direct benefit. Operative: may be problematic. Intelligence, simplicity.

Operatives may be most in need of training.

II) What training do the employees in your department currently have in DP?

None other than induction.

What methods are currently used for education and training within your department?

Induction, short training programs (vis, phys) for operative. Interactive/workshops for office.

Which of these methods are the most useful, which would you recommend for DPA education?

Interactive workshops for office. Understandable, practical, short, specific, clear for operative.

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…

Global e-mail=bad. Team meetings=good=effective. Notice boards are good supplements. Reminders are good. Manuals are ok if the info is concise and small, online would be good.

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?

Most data comes from [another dept] and is not maintained within the department. Sink of info is not controlled—operatives may retain info they should not have.

II) How do you protect individuals' data?

Are you letting employees and clients know about this?

III) What are the regulations on security? Access, taking information home

---

IV) Are you aware what will happen if someone wants to see the info held on them? Process and documentation

Personnel: if they come in they can see their file. There is no documented procedure. (clients' information is not kept in dept)

V) What means do you currently have to keep data up-to-date?
Do you have any policy for prevent the excessive retention of data?

Data is not kept up-to-date. There are only 2 people working there with too much to do. Insufficient resources not knowledge is the culprit.

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?

Simple q. Purpose and meaning, last application it was used for. Last training.

Interview #6

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?

Personal access requests were originally routed through [someone else], until Simon was appointed. Now, general questions are to Simon, and specific [departmental] advice goes to [other].

[Dept] holds more technical knowledge of the DPA98, is it part of their job.

What is the main effect (if any) of the DPA 98 on your department? How has the new law changed the way that things work? Changes in efficiency, office attitude, security…

No significant change that they're aware of. Did not begin at borough until after Act was implemented.

What are the greatest obstacles to compliance In your department?
Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…

The level of awareness of employees varies significantly between individuals. It is easier for [department] to comply, as it is part of their job.

II) What training do the employees in your department currently have in DP?

Some "in house" training sessions, some external courses (expensive; require individuals to leave for day).

What methods are currently used for education and training within your department?

(above)

Which of these methods are the most useful, which would you recommend for DPA education?

Employees like documents > a summary/agenda of the training/session could be given prior, followed by informal presentation/training session.

Presently have open-office like policy, allowing individuals with questions to ask managers

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…

Team meetings; (nothing else mentioned besides above). Like documents to read.

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?

Haven't yet implemented [specialized dept. system]. Certain methods- best filing review – improve service.

Personnel files – keep track of personnel files cupboard

II) How do you protect individuals' data?
Are you letting employees and clients know about this?
2 years ago, complaints about easy access into legal; back/fire door now locked preventing entrance from outside; developing limited access swipe system for main entrance

III) What are the regulations on security? Access, taking information home
----

IV) Are you aware what happens if someone wants to see the info held on them? Process and documentation
Not always dealt with properly. Could not handle if number of requests increased, as an individual has numerous files held on him, which takes a long time to compile and sort
Unsure of protocol, policy needed.
Need protocol for deletion of e-mail, "if you haven't got it, you can't give it"

V) What means do you currently have to keep data up-to-date?
Do you have any policy for prevent the excessive retention of data?
Up-to-date and excessive information is definitely a problem
There is no council-wide policy and there needs to be.
ie. Another company has been burning documents that are 20+ years old or 20+ years untouched, as they haven't been needed/used
Recommendation: periodic review, higher ups need to be involved
Suggestion: "Tidy Friday"
Increase litigious Increase requests.

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?
Prizes
- theatre tokens
- champagne
- gift vouchers for stores
- concert tickets

Charity fund > for each response, dept. donates to charity or something

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?
- criminal offence
- could you be in trouble with your professional body

Interview #7

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?
Deals with personal records ----

What is the main effect (if any) of the DPA 98 on your department? How has the new law changed the way that things work? Changes in efficiency, office attitude, security…
No changes whatsoever as result of DPA98. Lengthy absence of DP officer

Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…
What are the greatest obstacles to compliance In your department?
Employees are aware of the need for data protection and of the Act itself, but do not know of the content or any detail. No strategic development. No training

II) What training do the employees in your department currently have in DP?
None.

What methods are currently used for education and training within your department?
None.

Which of these methods are the most useful, which would you recommend for DPA education?
PowerPoint presentation, including overview of Act

- at different times of the day, allowing variety of employees to attend
- info session, 1 hour max.
- key questions for employees to take away and reflect upon
- corporate sessions
- joint training

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…

- Global e-mails aren't effective. But may send to an individual addressed as URGENT
- Individual e-mails will be paid attention to
- Elevator postings
- E-mails, communication from Chief Executives and Chief Officers – cascade
- "Flash messages"
  - on intranet
  - on computer desktops
  - on leaflet in with salary pay check
  - on message space on pay slip

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?

Information held between [2 departments] not linked to each other, not consistent. No way of tracking. Issue storage = lack of space.

II) How do you protect individuals' data?

Hold the files + kept in locked in files.

Are you letting employees and clients know about this?

III) What are the regulations on security? Access, taking information home

---

IV) Are you aware what will happen if someone wants to see the info held on them? Process and documentation

via appointment
Letter >> check out authenticity
*No written procedure

V) What means do you currently have to keep data up-to-date?
Do you have any policy for prevent the excessive retention of data?

Files on [certain individuals] kept 10 years after completion. Quite a bit of excess, out-of-date information. Results from lack of corporate initiative. Should be stored electronically or on microfilm; not enough funding for those methods. Most of budget goes toward paying staff salary, not toward projects

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

Discipline reaction. Negligence comes with penalties, responsibilities should be made clear. Should be linked with annual job appraisals. Should be written into job description.

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?

What do they know?
How do they carry it out?
What have they been asked which they don't know how to answer?

Interview #8

DEPARTMENTAL QUESTIONS

I) How do you feel that the DPA 98 applies to your department?

----.

What is the main effect (if any) of the DPA 98 on your department?

How has the new law changed the way that things work? Changes in efficiency, office attitude, security…

Does the average employee comply with DPA statutes? If not, why do you think that is? Procedure, time, perceived comparative importance…

People are aware of the DPA98 but unaware of what it asks. That why we have to work on training (guide)

What are the greatest obstacles to compliance In your department?

Not knowing how it applies to each situation. How it applied to them. Have a lot of info : Information internally and externally, care homes. Putting DPA clause into contacts. Access to info procedure not that good but will be better

II) What training do the employees in your department currently have in DP?

Has Internal training (induction) has to abide by the act so they can be aware o DPA and freedom of protection. But there will be more with the Caldicott. Increase training – quick guide for employees.

What methods are currently used for education and training within your department?

Team meeting which are 10 – 15 minutes where I talk to them and keep reminding them about a specific topic. Bigger in the induction. Newsletter. Global email. Ongoing thing. Not only one time. At lot of publicity.

Which of these methods are the most useful, which would you recommend for DPA education?

Typical person unaware of details o the 8 principles so we need to use– newsletter, Internet (internal), poster, email, guide (practical examples), and workshops session with practical examples saying what should be done or not.

III) What is the best form of intradepartmental communication? A newsletter, web page, team meetings…

Newsletter. Reminders in staff meetings, and emails reminders. Send constants reminders, regular feedback (face to face)

EIGHT PRINCIPLES

I) Is there some way to track the flow of information? How can you tell where your information came from (department)? How can you make sure that it is not transferred to inappropriate places?

Information flow is problematic. Need of protocol. If you look at each individual record, you can tell where it came from and where it went, but there is no overall schematic showing the flow of information.

II) How do you protect individuals' data?

BSI security, every computer/database is password protected, with different levels of access. Hard copies are not as well protected.

Are you letting employees and clients know about this?

III) What are the regulations on security? Access, taking information home

Files are not allowed to be taken home—have policy but there is no real enforcement of this.

IV) Are you aware what will happen if someone wants to see the info held on them? Process and documentation

There is a procedure which is under review.

V) What means do you currently have to keep data up-to-date?

Case files reviewed at end and at beginning by the social workers

VI) What do you feel would be an effective and appropriate incentive for compliance for people in your department?

Newsletter and quiz questions.

VII) Would there be any specific question you have that you would like to ask your personnel in a survey?

<u>SENSITIVE DATA</u>

I) Here are some examples of sensitive data: racial origin, ethnicity, politics, beliefs, health, sexual preferences, criminal charges and convictions.

II) Do you take special precautions with sensitive data that you possess? What are they?

[Certain divisions] have a higher care. Higher awareness.

Appendix G: Survey Disclaimer

YOU CAN WIN £20
IN 10 MINUTES!

We are conducting a survey on data protection awareness. We are working with the Data Protection Officer to create a program that will help you to understand the practical implications of the Data Protection Act. Your response to this survey is important, as it will aid in determining areas in need of further data protection training and policy.

The survey will be completely anonymous and your responses will be neither tracked nor passed on. Do not be concerned with choosing the "correct" answer, as your perceptions are more valued. It should take you less than 10 minutes to complete the survey.

Upon completing the survey, you will be given a randomly generated number. This number is your raffle ticket for a gift voucher. If you complete the survey by February 6, you are eligible to win one of three £5 vouchers. If you reply by January 31, you are also eligible to win a £20 voucher. Please send an e-mail including your number to ce_wpis@merton.gov.uk if you wish to enter the drawing. The owner of the winning number will be contacted February 7, via the e-mail address he or she provides.

Appendix H: Online Survey Template

1. What division are you currently working in (optional):

.....

2. How would you describe your position?

- ◉ Managerial
- ○ Non-Managerial

.....

3. How would you describe your knowledge of the Data Protection Act of 1998?

- ○ In-depth
- ○ General awareness, but not of details
- ○ Not really knowledgeable

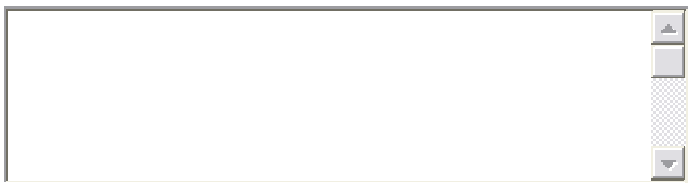
.....

4. Please rate how you feel towards the following training methods for Data Protection.

	Prefer	Neutral	Dislike
Manuals	○	○	○
Posters	○	○	○
Pamphlets	○	○	○
Seminars	○	○	○
Work during team meetings	○	○	○

.....

5. Please state any ideas you have for possible training regarding the Data Protection Act of 1998 for your specific department.



.....

6. How long has it been since your last training on the DPA 98?

- Less than 6 Months
- Less then 1 Year
- Less then 2 Years
- Not Since Induction
- Never

.....

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?

- Nobody
- Department head
- Co-workers in division
- Data Protection Officer

.....

8. When should you contact the Data Protection officer? Choose all that apply.

- Never directly
- Only in an emergency
- When your manager tells you to
- When you have a question about Data Protection
- Whenever you are bored

.....

9. What happens if you don't reply to an individual's personal data request? Choose all that apply.

- Nothing
- Verbal reprimand from supervisor
- Loss of employment
- Penalty under law

.....

10. How many times per week does the DPA 98 affect your work?

- None
- Once
- Twice

- Three Times
- More then Three Times

.....

The following questions propose some basic situations concerning personal data protection, please answer then as honestly as possible, without consulting any informative material, or asking someone else. Honest answers to these questions will help us to gain a better understanding as to the difficult areas o the act itself.

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?

- 30 Calendar Days
- 30 Working Days
- 40 Calendar Days
- 40 Working Days
- 60 Calendar Days

.....

12. I've got a personal database on my computer at work. It's not an official system, in fact only I know about it. I use it to keep details of clients who have caused me difficulties in the past so I can treat them with kid gloves next time. Do you think this is ok?

- Yes
- No

.....

13. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?

- Yes
- No

.....

14. Someone's just called up one of my team and has demanded to see all the information we hold on them. What should I do?

->

.....

16. Please use the following responses to answer how you feel about the next four statements.

	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
It takes too much time to follow the DPA.					
Following DPA regulations is as important.					
The DPA is effective for protection of personal information.					
The information I work with to is not subject to DPA standards.					

.....
Thank you once gain for taking the time to fill out our survey! Here is your number, please take it down, enter it into the SUBJECT line of an e-mail addressed to ce_wpis@merton.gov.uk in order to have your chance at 20 quid!

Your Number --->

Submit Survey

Powered by SurveySolutions XP web survey software

Appendix I: Housing and Social Services Survey

1. What division are you currently working in *(optional)*:
   (Free entry field)_____

2. How would you describe your position?

Managerial	Non-Managerial

3. How would you describe your knowledge of the Data Protection Act of 1998?
   In-depth___ General awareness, but not of details___
   Not really knowledgeable___

4. Please rate your feelings toward the following training methods, using the choices below.
   1: Dislike
   2: Neutral
   3: Prefer

   Manuals: _____
   Posters: _____
   Pamphlets: _____
   Seminars: _____
   Work during team meetings: _____

5. State any ideas for possible training regarding the DPA 98 for your specific department
   (Free Entry Field)

6. How long has it been since your last training on the DPA 98?
   __ Less than 6 months
   __ Less than one year
   __ Less than two years
   __ Not since induction
   __ Never

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?
   __ Nobody
   __ Department head
   __ Co-workers in division
   __ Data Protection Officer

8. When should you contact the Data Protection officer?
   __ Never directly
   __ Only in an emergency
   __ When your manager tells you to
   __ When you have a question about Data Protection

__ Whenever you are bored

9. What happens if you don't reply to an individual's personal data request?
__ Nothing
__ Verbal reprimand from supervisor
__ Loss of employment
__ Penalty under law

10. How many times per week does the DPA 98 affect your work?
__None __Once __Twice __Three Times __More then 3 Times

The following questions propose some basic situations concerning data protection. Please answer then as honestly as possible, without consulting any informative material, or asking someone else. Honest answers to these questions will better help us difficult areas of data protection.

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him. How long do you feel is an appropriate amount of time in which to supply this information?
30 Calendar Days __
30 Working Days __
40 Calendar Days__
40 Working Days __
60 Calendar Days__

12. A parent calls and asks for all the information you hold on her child. This child is a special education student and there have been calls to social services about potential abuse. While going through this child's file you notice that it indicates the person that notified social services about the child's situation. What would you do?
___Give parent all the information
___Give parent partial information
___Give parent no information

13. After you have completed a packet, which is to be mailed to a citizen requesting information, you notice that there is quite a lot of information being held that is no longer necessary, or clearly out of date. What do you feel contributed the most to this occurring?
Lack of resources ___
Poor training on data protection ___
Improper handling of files ___

14. I've got a personal database on my computer at work. It's not an official system, in fact only I know about it. I use it to keep details of clients who have caused me difficulties in the past so I can treat them with kid gloves next time. Do you think this is ok?
__ Yes __ No

15. Please use the following responses to answer how you feel about the next four statements.

1 – Strongly Agree
2 – Agree
3 – Don't care / no opinion
4 - Disagree
5 – Strongly disagree

a) It requires too much time to follow DPA regulations. _____
b) Following DPA regulations is as important as the rest of my work. _____
c) The DPA 1998 is an effective means of protecting personal information._____
d) The information to which I have access is not important enough to be protected. _____

Appendix J: Leisure, Library and Education Survey

1. What division are you currently working in *(optional)*:
   (Free entry field)_____

2. How would you describe your position?

Managerial	Non-Managerial

3. How would you describe your knowledge of the Data Protection Act of 1998?
   In-depth___ General awareness, but not of details___
   Not really knowledgeable___

4. Please rate your feelings toward the following training methods, using the choices below.
   1: Dislike
   2: Neutral
   3: Prefer

   Manuals: _____
   Posters: _____
   Pamphlets: _____
   Seminars: _____
   Work during team meetings: _____

5. State any ideas for possible training regarding the DPA 98 for your specific department
   (Free Entry Field)

6. How long has it been since your last training on the DPA 98?
   __ Less than 6 months
   __ Less than one year
   __ Less than two years
   __ Not since induction
   __ Never

7. You receive a phone call or letter requesting from an individual requesting information about himself. Who would you notify?
   __ Nobody
   __ Department head
   __ Co-workers in division
   __ Data Protection Officer

8. When should you contact the Data Protection officer?
   __ Never directly
   __ Only in an emergency
   __ When your manager tells you to
   __ When you have a question about Data Protection

__ Whenever you are bored

9. What happens if you don't reply to an individual's personal data request?
__ Nothing
__ Verbal reprimand from supervisor
__ Loss of employment
__ Penalty under law

10. How many times per week does the DPA 98 affect your work?
__None __Once __Twice __Three Times __More then 3 Times

The following questions propose some basic situations concerning data protection. Please answer then as honestly as possible, without consulting any informative material, or asking someone else. Honest answers to these questions will better help us difficult areas of data protection.

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?
30 Calendar Days __
30 Working Days __
40 Calendar Days__
40 Working Days __
60 Calendar Days__

12. I've got a personal database on my computer at work. It's not an official system, in fact only I know about it. I use it to keep details of clients who have caused me difficulties in the past so I can treat them with kid gloves next time. Do you think this is ok?
__ Yes __ No

13. An individual calls demanding to know what address we have been sending correspondence addressed to him to. What course of action do you take?
__ Ask what address he thinks it might be
__ Tell him the address on file
__ Ask him to come in with proof of ID to discuss the issues

14. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?
__ Yes __ No

15. Please use the following responses to answer how you feel about the next four statements.

1 – Strongly Agree
2 – Agree
3 – Don't care / no opinion
4 - Disagree
5 – Strongly disagree

a) It requires too much time to follow DPA regulations. _____

b) Following DPA regulations is as important as the rest of my work. _____
c) The DPA 1998 is an effective means of protecting personal information._____
d) The information to which I have access is not important enough to be protected. _____

Appendix K: Environmental Survey

1. What division are you currently working in *(optional)*:
   (Free entry field)_____

2. How would you describe your position?

Managerial	Non-Managerial

3. How would you describe your knowledge of the Data Protection Act of 1998?
   In-depth___ General awareness, but not of details___
   Not really knowledgeable___

4. Please rate your feelings toward the following training methods, using the choices below.
   1: Dislike
   2: Neutral
   3: Prefer

   Manuals: _____
   Posters: _____
   Pamphlets: _____
   Seminars: _____
   Work during team meetings: _____

5. State any ideas for possible training regarding the DPA 98 for your specific department
   (Free Entry Field)

6. How long has it been since your last training on the DPA 98?
   __ Less than 6 months
   __ Less than one year
   __ Less than two years
   __ Not since induction
   __ Never

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?
   __ Nobody
   __ Department head
   __ Co-workers in division
   __ Data Protection Officer

8. When should you contact the Data Protection officer?
   __ Never directly
   __ Only in an emergency
   __ When your manager tells you to
   __ When you have a question about Data Protection

__ Whenever you are bored

9. What happens if you don't reply to an individual's personal data request?
__ Nothing
__ Verbal reprimand from supervisor
__ Loss of employment
__ Penalty under law

10. How many times per week does the DPA 98 affect your work?
__None __Once __Twice __Three Times __More then 3 Times

11. Typically how long do you keep files you are using on your desk?
__ 1 hour __ 1 day __ 1 week __ 1 month __ indefinite

12. Do you know how to password a file on your computer?
__ Yes __ No

The following questions propose some basic situations concerning data protection. Please answer then as honestly as possible, without consulting any informative material, or asking someone else. Honest answers to these questions will better help us difficult areas of data protection.

13. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?
30 Calendar Days __
30 Working Days __
40 Calendar Days__
40 Working Days __
60 Calendar Days__

14. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?
__ Yes __ No

15. A manager from financial services comes to your desk one afternoon. He is in immediate need of the information you hold on one of your clients. He is in a rush and up against a deadline. What do you do?

___ Give him the entire file he wants.
___ Ask him why he needs it, sort through the files and give what you think is necessary.
___ Refuse all information.

16. Please use the following responses to answer how you feel about the next four statements.

1 – Strongly Agree
2 – Agree
3 – Don't care / no opinion
4 - Disagree
5 – Strongly disagree

a) It requires too much time to follow DPA regulations. _____
b) Following DPA regulations is as important as the rest of my work. _____
c) The DPA 1998 is an effective means of protecting personal information._____
d) The information to which I have access is not important enough to be protected. _____

Appendix L: Finance Survey

1. What division are you currently working in *(optional)*:
(Free entry field)_____

2. How would you describe your position?

Managerial	Non-Managerial

3. How would you describe your knowledge of the Data Protection Act of 1998?
In-depth___ General awareness, but not of details___
Not really knowledgeable___

4. Please rate your feelings toward the following training methods, using the choices below.
1: Dislike
2: Neutral
3: Prefer

Manuals: _____
Posters: _____
Pamphlets: _____
Seminars: _____
Work during team meetings: _____

5. State any ideas for possible training regarding the DPA 98 for your specific department
(Free Entry Field)

6. How long has it been since your last training on the DPA 98?
__ Less than 6 months
__ Less than one year
__ Less than two years
__ Not since induction
__ Never

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?
__ Nobody
__ Department head
__ Co-workers in division

__ Data Protection Officer

8. When should you contact the Data Protection officer?
__ Never directly
__ Only in an emergency
__ When your manager tells you to
__ When you have a question about Data Protection
__ Whenever you are bored

9. What happens if you don't reply to an individual's personal data request?
__ Nothing
__ Verbal reprimand for supervisor
__ Loss of employment
__ Penalty under law

10. How many times per week does the DPA 98 affect your work?
__None __Once __Twice __Three Times __More then 3 Times

The following questions propose some basic situations concerning data protection. Please answer then as honestly as possible, without consulting any informative material, or asking someone else. Honest answers to these questions will better help us difficult areas of data protection.

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?
30 Calendar Days __
30 Working Days __
40 Calendar Days__
40 Working Days __
60 Calendar Days__

17. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?
__ Yes __ No

18. One individual on housing benefit is a constant source of problems for your department. This time he has lost his rent cheque. His landlord, confused about the lack of payment, contacts you to ask you what is going on. What do you do?

___Explain the situation
___Evade the question
___Refuse information

19. A woman from Housing and Social Services comes over to ask you about an individual. She is rushed and up against a deadline. She tells you that Housing and Social Services has misplaced his file and would like to borrow the file you have on him. What would you do?

___Give her his entire file
___Ask why she needs the information and give her what you feel is appropriate
___Refuse to give her information

20. Please use the following responses to answer how you feel about the next four statements.

1 – Strongly Agree
2 – Agree
3 – Don't care / no opinion
4 - Disagree
5 – Strongly disagree

a) It requires too much time to follow DPA regulations. _____
b) Following DPA regulations is as important as the rest of my work. _____
c) The DPA 1998 is an effective means of protecting personal information._____
d) The information to which I have access is not important enough to be protected. _____

Appendix M: Chief Executive Survey

1. What division are you currently working in *(optional)*:
   (Free entry field)_____

2. How would you describe your position?

Managerial	Non-Managerial

3. How would you describe your knowledge of the Data Protection Act of 1998?
   In-depth___ General awareness, but not of details___
   Not really knowledgeable___

4. Please rate your feelings toward the following training methods, using the choices below.
   1: Dislike
   2: Neutral
   3: Prefer

   Manuals: _____
   Posters: _____
   Pamphlets: _____
   Seminars: _____
   Work during team meetings: _____

5. State any ideas for possible training regarding the DPA 98 for your specific department
   (Free Entry Field)

6. How long has it been since your last training on the DPA 98?
   __ Less than 6 months
   __ Less than one year
   __ Less than two years
   __ Not since induction
   __ Never

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?
   __ Nobody
   __ Department head
   __ Co-workers in division
   __ Data Protection Officer

8. When should you contact the Data Protection officer?
   __ Never directly
   __ Only in an emergency
   __ When your manager tells you to
   __ When you have a question about Data Protection

__ Whenever you are bored

9. What happens if you don't reply to an individual's personal data request?
__ Nothing
__ Verbal reprimand from supervisor
__ Loss of employment
__ Penalty under law

10. How many times per week does the DPA 98 affect your work?
__None __Once __Twice __Three Times __More then 3 Times

The following questions propose some basic situations concerning data protection. Please answer then as honestly as possible, without consulting any informative material, or asking someone else. Honest answers to these questions will better help us difficult areas of data protection.

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?
30 Calendar Days __
30 Working Days __
40 Calendar Days__
40 Working Days __
60 Calendar Days__

12. I've got a personal database on my computer at work. It's not an official system, in fact only I know about it. I use it to keep details of clients who have caused me difficulties in the past so I can treat them with kid gloves next time. Do you think this is ok?
__ Yes __ No

13. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?
__ Yes __ No

14. Someone's just called up one of my team and has demanded to see all the information we hold on them. What should I do?
(Free entry field)_____

15. Please use the following responses to answer how you feel about the next four statements.

1 – Strongly Agree	4 - Disagree
2 – Agree	5 – Strongly disagree
3 – Don't care / no opinion	

a) It requires too much time to follow DPA regulations. _____
b) Following DPA regulations is as important as the rest of my work. _____
c) The DPA 1998 is an effective means of protecting personal information._____

d) The information to which I have access is not important enough to be protected. _____

Appendix N: Survey Results

Chief Executive

2. How would you describe your position?

Choice	Count	Percentage
Managerial	14	25%
Non-Managerial	42	75%

3. How would you describe your knowledge of the Data Protection Act of 1998?

Choice	Count	Percentage
In-depth	6	11%
General awareness, but not of details	37	66%
Not really knowledgeable	13	23%

4. Please rate how you feel towards the following training methods for Data Protection.

Topic	Prefer	Neutral	Dislike
Manuals	19	20	15
Posters	16	26	11
Pamphlets	32	19	5
Seminars	29	18	8
Work during team meetings	21	29	4

6. How long has it been since your last training on the DPA 98?

Choice	Count	Percentage
Less than 6 Months	10	18%
Less then 1 Year	1	2%
Less then 2 Years	3	5%
Not Since Induction	4	7%
Never	38	68%

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?

Choice	Count
Nobody	3
Department head	2
Co-workers in division	6
Line Manager	31
Data Protection Officer	14

8. When should you contact the Data Protection officer? Choose all that apply.

Choice	Count
Never directly	0
Only in an emergency	1
When your manager tells you to	11
When you have a question about Data Protection	21
Whenever you are bored	0

9. What happens if you don't reply to an individual's personal data request? Choose all that apply.

Choice	Count
Nothing	8
Verbal reprimand from supervisor	18
Loss of employment	3
Penalty under law	41

10. How many times per week does the DPA 98 affect your work?

Choice	Count	Percentage
None	8	14%
Once	7	13%
Twice	3	5%
Three Times	0	0%
More then Three Times	13	23%
I Don't Know	25	45%

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?

Choice	Count	Percentage
30 Calendar Days	26	49%
30 Working Days	18	33%
40 Calendar Days	4	7%
40 Working Days	2	4%
60 Calendar Days	4	7%

12. I've got a personal database on my computer at work. It's not an official system, in fact only I know about it. I use it to keep details of clients who have caused me difficulties in the past so I can treat them with kid gloves next time. Do you think this is ok?

Choice	Count	Percentage
Yes	11	80%
No	45	20%

13. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?

Choice	Count	Percentage
Yes	2	4%
No	54	96%

15. Please use the following responses to answer how you feel about the next four statements.

Topic	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
It takes too much time to follow the DPA.	3	5	29	15	3
Following DPA regulations is as important as my other work.	11	25	12	6	1
The DPA is effective for protection of personal information.	9	27	16	3	0
The information I work with to is not subject to DPA standards.	1	3	15	23	14

Education, Leisure and Libraries

2. How would you describe your position?

Choice	Count	Percentage
Managerial	15	39%
Non-Managerial	23	61%

3. How would you describe your knowledge of the Data Protection Act of 1998?

Choice	Count	Percentage
In-depth	1	5%
General awareness, but not of details	13	61%
Not really knowledgeable	8	34%

4. Please rate how you feel towards the following training methods for Data Protection.

Topic	Prefer	Neutral	Dislike
Manuals	11	15	10
Posters	5	19	10
Pamphlets	13	20	3
Seminars	17	13	7
Work during team meetings	20	8	9

6. How long has it been since your last training on the DPA 98?

Choice	Count	Percentage
Less than 6 Months	0	0%
Less then 1 Year	0	0%
Less then 2 Years	1	3%
Not Since Induction	1	3%
Never	36	94%

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?

Choice	Count
Nobody	2
Department head	5
Co-workers in division	1
Line Manager	21
Data Protection Officer	8

8. An employer calls requesting information on a job applicant. How much information do you give him? Choose all that apply.

Choice	Count
Financial status	0

Criminal record	0
Employment history	18
None	20

9. When should you contact the Data Protection officer? Choose all that apply.

Choice	Count
Never directly	2
Only in an emergency	3
When your manager tells you to	19
When you have a question about Data Protection	31
Whenever you are bored	1

10. What happens if you don't reply to an individual's personal data request? Choose all that apply.

Choice	Count
Nothing	10
Verbal reprimand from supervisor	4
Loss of employment	0
Penalty under law	21

11. How many times per week does the DPA 98 affect your work?

Choice	Count	Percentage
None	7	18%
Once	2	5%
Twice	1	3%
Three Times	0	0%
More then Three Times	5	13%
I Don't Know	23	61%

12. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?

Choice	Count	Percentage
30 Calendar Days	25	68%
30 Working Days	10	27%
40 Calendar Days	2	5%
40 Working Days	0	0%
60 Calendar Days	0	0%

13. An individual calls demanding to know what address we have been sending correspondence addressed to him to. What course of action do you take?

Choice	Count	Percentage
Ask what address he thinks it might be.	19	51%
Tell him the address on file.	1	46%

Ask him to come in with proof of ID to discuss the issues.	17	3%

14. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?

Choice	Count	Percentage
Yes	1	2%
No	40	98%

15. Please use the following responses to answer how you feel about the next four statements.

Topic	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
It requires too much time to follow DPA regulations.	0	1	12	7	1
Following DPA regulations is as important as the rest of my work.	2	8	8	1	2
The DPA 1998 is an effective means of protecting personal information.	0	10	8	2	2
The information to which I have access is not important enough to be protected.	0	4	2	12	4

Environmental Services

2. How would you describe your position?

Choice	Count	Percentage
Managerial	13	42%
Non-Managerial	18	58%

3. How would you describe your knowledge of the Data Protection Act of 1998?

Choice	Count	Percentage
In-depth	3	10%
General awareness, but not of details	24	77%
Not really knowledgeable	4	13%

4. Please rate how you feel towards the following training methods for Data Protection.

Topic	Prefer	Neutral	Dislike
Manuals	14	8	9
Posters	6	15	9
Pamphlets	12	15	3
Seminars	17	11	1
Work during team meetings	13	11	6

6. How long has it been since your last training on the DPA 98?

Choice	Count	Percentage
Less than 6 Months	5	16%
Less then 1 Year	0	0%
Less then 2 Years	1	3%
Not Since Induction	2	6%
Never	23	75%

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?

Choice	Count	Percentage
Nobody	2	6%
Department head	2	6%
Co-workers in division	0	0%
Line Manager	18	59%
Data Protection Officer	9	29%

8. When should you contact the Data Protection officer? Choose all that apply.

Choice	Count
Never directly	0
Only in an emergency	4
When your manager tells you to	11
When you have a question about Data Protection	28
Whenever you are bored	0

9. What happens if you don't reply to an individual's personal data request? Choose all that apply.

Choice	Count
Nothing	5
Verbal reprimand from supervisor	11
Loss of employment	3
Penalty under law	15

10. How many times per week does the DPA 98 affect your work?

Choice	Count	Percentage
None	5	17%
Once	4	13%
Twice	2	7%
Three Times	0	0%
More then Three Times	8	27%
I don't know	11	36%

11. Typically how long do you keep files you are using on your desk?

Choice	Count	Percentage
1 hour	3	10%
1 day	6	19%
1 week	5	16%
1 month	7	23%
indefinite	10	32%

12. Do you know how to password a file on your computer?

Choice	Count	Percentage
Yes	16	53%
No	14	47%

13. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?

Choice	Count	Percentage
30 Calendar Days	13	43%
30 Working Days	11	35%
40 Calendar Days	3	10%
40 Working Days	2	6%
60 Calendar Days	2	6%

14. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?

Choice	Count	Percentage

Yes	0	0%
No	31	100%

15. A manager from financial services comes to your desk one afternoon. He is in immediate need of the information you hold on one of your clients. He is in a rush and up against a deadline. What do you do?

Choice	Count	Percentage
Give him the entire file he wants.	2	7%
Ask him why he needs it, sort through the files and give what you think is necessary.	19	63%
Refuse all information.	9	30%

16. Please use the following responses to answer how you feel about the next four statements.

Topic	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
It requires too much time to follow DPA regulations.	0	5	17	9	0
Following DPA regulations is as important as the rest of my work.	4	13	10	3	0
The DPA 1998 is an effective means of protecting personal information.	4	18	6	2	0
The information to which I have access is not important enough to be protected.	0	7	7	15	1

Finance

2. How would you describe your position?

Choice	Count
Managerial	14
Non-Managerial	19

3. How would you describe your knowledge of the Data Protection Act of 1998?

Choice	Count	Percentage Answered
In-depth	2	4.50%
General awareness, but not of details	28	81.80%
Not really knowledgeable	3	13.60%

4. Please rate how you feel towards the following training methods for Data protection.

Manuals	19	7	5
Posters	8	15	5
Pamphlets	12	14	0
Seminars	19	10	2
Work during team meetings	9	12	6
Manuals	19	7	5

6. How long has it been since your last training on the DPA 98?

Choice	Count
Less than 6 Months	1
Less then 1 Year	5
Less then 2 Years	5
Not Since Induction	7
Never	15

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?

Choice	Count
Nobody	7
Department head	1
Co-workers in division	2
Line Manager	13
Data Protection Officer	10

8. When should you contact the Data Protection officer? Choose all that apply.

Choice	Count
Never directly	3
Only in an emergency	1
When your manager tells you to	12
When you have a question about Data Protection	27

Whenever you are bored	0

9. What happens if you don't reply to an individual's personal data request? Choose all that apply.

Choice	Count
Nothing	6
Verbal reprimand from supervisor	6
Loss of employment	0
Penalty under law	20

10. How many times per week does the DPA 98 affect your work?

Choice	Count
None	9
Once	1
Twice	0
Three Times	0
More then Three Times	15
I don't know	8

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?

Choice	Count
30 Calendar Days	19
30 Working Days	10
40 Calendar Days	1
40 Working Days	3
60 Calendar Days	0

12. My best friend from school still lives in the area. Can I use our database to have a quick look to see where she's living now?

Choice	Count
Yes	1
No	32

13. One individual on housing benefit is a constant source of problems for your department. This time he has lost his rent cheque. His landlord, confused about the lack of payment, contacts you to ask you what is going on. What do you do?

Choice	Count
Explain the situation	8
Evade the question	0
Refuse information	24

14. A woman from Housing and Social Services comes over to ask you about an individual. She is rushed and up against a deadline. She tells you that Housing and Social Services has misplaced his file and would like to borrow the file you have on him. What would you do?

Choice	Count
Give her his entire file	0
Ask why she needs the information and give her what you feel is appropriate	25
Refuse to give her information	8

16. Please use the following responses to answer how you feel about the next four statements.

Topic	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
It requires too much time to follow DPA regulations.	1	2	10	19	0
Following DPA regulations is as important as the rest of my work.	8	17	6	2	0
The DPA 1998 is an effective means of protecting personal information.	5	20	5	3	0
The information to which I have access is not important enough to be protected.	0	2	5	16	9

Housing and Social Services

2. How would you describe your position?

Choice	Count	Percentage
Managerial	24	30%
Non-Managerial	55	70%

3. How would you describe your knowledge of the Data Protection Act of 1998?

Choice	Count	Percentage
In-depth	2	3%
General awareness, but not of details	59	73%
Not really knowledgeable	19	24%

4. Please rate how you feel towards the following training methods for Data Protection.

Topic	Prefer	Neutral	Dislike
Manuals	30	28	18
Posters	22	40	13
Pamphlets	44	28	4
Seminars	43	28	6
Work during team meetings	31	35	11

6. How long has it been since your last training on the DPA 98?

Choice	Count	Percentage
Less than 6 Months	5	6%
Less then 1 Year	1	0%
Less then 2 Years	5	6%
Not Since Induction	5	6%
Never	63	81%

7. You receive a phone call or letter from an individual requesting information about himself. Who would you notify?

Choice	Count
Nobody	9
Department head	5
Co-workers in division	8
Line Manager	45
Data Protection Officer	13

8. When should you contact the Data Protection officer? Choose all that apply.

Choice	Count
Never directly	3
Only in an emergency	3
When your manager tells you to	46
When you have a question about Data Protection	63

Whenever you are bored	0

9. What happens if you don't reply to an individual's personal data request? Choose all that apply.

Choice	Count
Nothing	10
Verbal reprimand from supervisor	35
Loss of employment	5
Penalty under law	47

10. How many times per week does the DPA 98 affect your work?

Choice	Count	Percentage
None	12	16%
Once	10	13%
Twice	1	4%
Three Times	4	5%
More then Three Times	26	34%
I don't know	24	31%

11. You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?

Choice	Count
30 Calendar Days	33
30 Working Days	35
40 Calendar Days	6
40 Working Days	4
60 Calendar Days	2

12. A parent calls and asks for all the information you hold on her child. This child is a special education student and there have been calls to social services about potential abuse. While going through this child's file you notice that it indicates the person that notified social services about the child's situation. What would you do?

Choice	Count	Percentage
Give parent all the information	3	4%
Give parent partial information	41	51%
Give parent no information	36	45%

13. After you have completed a packet, which is to be mailed to a citizen requesting information, you notice that there is quite a lot of information being held that is no longer necessary, or clearly out of date. What do you feel contributed the most to this occurring?

Choice	Count	Percentage

Lack of resources	12	15%
Poor training on data protection	29	37%
Improper handling of files	37	48%

14. I've got a personal database on my computer at work. It's not an official system, in fact only I know about it. I use it to keep details of clients who have caused me difficulties in the past so I can treat them with kid gloves next time. Do you think this is ok?

Choice	Count	Percentage
Yes	8	10%
No	69	90%

15. Please use the following responses to answer how you feel about the next four statements.

Topic	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
It requires too much time to follow DPA regulations.	1	13	29	28	6
Following DPA regulations is as important as the rest of my work.	17	44	9	6	1
The DPA 1998 is an effective means of protecting personal information.	13	47	12	7	0
The information to which I have access is not important enough to be protected.	2	4	6	36	29

Survey Results: All Surveys

How would you describe your position?

Choice	Count	Percentage
Managerial	80	34%
Non-Managerial	157	66%

How would you describe your knowledge of the Data Protection Act of 1998?

Choice	Count	Percentage
In-depth	14	6%
General awareness, but not of details	161	73%
Not really knowledgeable	47	21%

Please rate how you feel towards the following training methods for Data Protection.

Topic	Prefer	Neutral	Dislike
Manuals	93	78	57
Posters	57	115	48
Pamphlets	113	96	15
Seminars	125	80	24
Work during team meetings	94	95	36

How long has it been since your last training on the DPA 98?

Choice	Count	Percentage
Less than 6 Months	21	9%
Less then 1 Year	7	3%
Less then 2 Years	15	6%
Not Since Induction	19	8%
Never	175	74%

You receive a phone call or letter from an individual requesting information about himself. Who would you notify?

Choice	Count
Nobody	23
Department head	15
Co-workers in division	17
Line Manager	128
Data Protection Officer	54

When should you contact the Data Protection officer? Choose all that apply.

Choice	Count
Never directly	8
Only in an emergency	12

When your manager tells you to	99
When you have a question about Data Protection	170
Whenever you are bored	1

What happens if you don't reply to an individual's personal data request? Choose all that apply.

Choice	Count
Nothing	39
Verbal reprimand from supervisor	74
Loss of employment	11
Penalty under law	144

How many times per week does the DPA 98 affect your work?

Choice	Count	Percentage
None	41	18%
Once	24	10%
Twice	7	3%
Three Times	4	2%
More then Three Times	67	29%
I Don't Know	91	38%

You are given a letter from the Data Protection Officer. The letter is a request from a concerned citizen, whose identity has been confirmed, requesting all the information that your department holds on him, how long do you feel is an appropriate amount of time in which to supply this information?

Choice	Count
30 Calendar Days	116
30 Working Days	84
40 Calendar Days	16
40 Working Days	11
60 Calendar Days	8

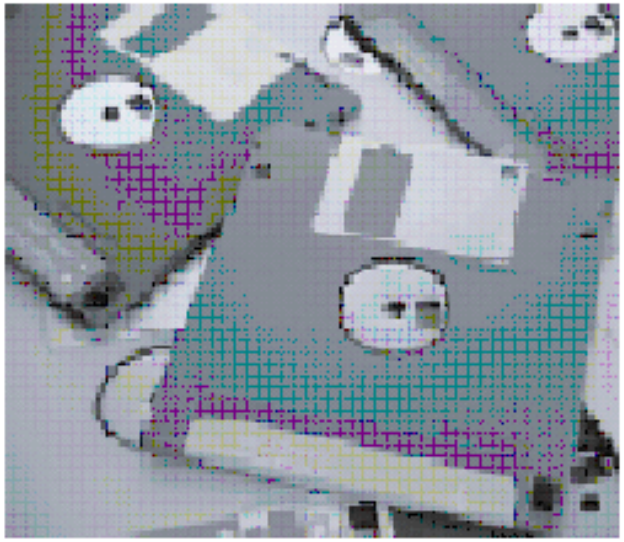
Please use the following responses to answer how you feel about the next four statements.

Topic	Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
It requires too much time to follow DPA regulations.	5	26	97	78	10
Following DPA regulations is as important as the rest of my work.	42	107	45	18	4
The DPA 1998 is an effective means of protecting personal information.	31	122	47	17	2
The information to which I have access is not important enough to be protected.	3	20	35	102	57

Education/Training				
	Do you have training?	**Current training methods**	**Training methods you recommend**	**Interdepartamental communication**
Chief Executive	none	invited Simon Guild for session. No corporate training	team meetings - smaller groups, open forms, notes on lifts, notice boards, reminders. Reinforce/remind i.e "Did you know.."	team meetings
	some "in house" sessions, some external courses (expensive; require individuals to leave for day	some "in house" sessions, some external courses (expensive; require individuals to leave for day	lawyers like document - summary/ agenda o the training/session could be given prior followed by inormal presentatn.training sessio. Open office - policy	team meetings (lawyers like documents to read)
Housing and Social Services	internatl training (induction) - so can be aware of DPA98 and freedom of protection - more w/ Caldicott	team meeting (10-15 minutes) , newsletter, global email, ongoing thing	newsletter, internet (internal), poster, email, guide (pratical examples), and workshop sessions with pratical example of what should be done or not	newsletter, reminders inn staff meeting, and emial reminders. Send constant reminders, regular feedback (face to face)
	training seminars every 6 weeks, may be on DP. Have long been subject to Caldicott. Trained in infotn gathering and recording.	training days every 6 weeks, monthly staff meetings, intitial induction	briefings, repetition, 5 times, re-tell when return, reminders by email	staff meetings - team managers should trickle down, Intranet policiews I confusing, use seminars - should be interactive
Finance	everyone trained in DPA before entry, seminars	manual for evrybody - coaching for grade B - manual updated - training or specific issues	posters/ bulletins are bad - no one reads them. Specific training courses is good. Global emails sometimes work	heads o services meeting, 0.5-1.0 day, infotn dispersed through team meetings
Environmental Service	none, other than induction	induction, short training program (vis, phys) or operative. Interactive/workshops for ofice	interactive workshops for office. Understandable, pratical, short, specific, clear for operative	global email = bad. Team meeting = good. Notice boards are good supplement. Reminders are good. Manuals are ok if the infotn is concise and small, online would be good.
	NA	NA	two levels - one - resources for employees, written notes, handbooks, guides to refer to. Two - training specifics to individuals, no blanket training, pratical.	team meetings, not e-mail. Third and 4th tier were most useful for training, trickle down doesn't always work, operatives don't always get info.
Education, Leisure, and Library	none	none	Powerpoint presentation, including overview of Act: different times of the day, allowing variety of employees to attend (i.e: teachers), info session -1 hr max, key questions for employees to take away and reflect upon, corporate sessions, joint-training-social services-individual families	Global emails aren't effective. But may send to an individual addressed as urgent, individual emails will be paid attention to. Elevator postings, emails - hierachy cascade, "flash messages" (intranet, computer dektop, lealet in w/ salary packet on message space of the pay slip)

Appendix P: Sample Posters

Data protection is everyone's job



A man was sure his girlfriend was cheating on him. He convinced two employees of the O2 mobile phone company to forward her incriminating text messages to him. With his new proof he was even more infuriated. In revenge, he posted explicit pictures of himself and the girl on a website and sent all the girl's friends links to the site.

Maybe it's obvious that you have to be careful of who you give to, but even other Council employees can't be given information without a need for it.

Appendix Q: Sample Payslip Attachments

Make sure the personal information you're responsible for is up to date!

Make sure to lock your computer with a password every time you leave your desk. Data protection is everyone's job.

Is there too much information in your files? Make an effort to neaten up those files!

Have a question about Data Protection? Contact Merton's Data Protection Officer, Mr. Simon Guild at x4182. Better to ask a question then break the law.

Individuals now have to right to see the information the borough holds on them, so long as it doesn't reveal any information about another individual. The borough has 40 calendar days to send this information to the individual to stay within the law.

Data Protection—it may be a pain, but it's also the law.

Would you like convicted sex offenders to have easy access to your home address and phone numbers? Of course not. Data Protection is important, and it's the law.

Would you like a con man to have easy access to your personal information? No? Keep personal information secure, follow the Data Protection Act to the letter of the Law.

Do your files contain old or irrelevant information? If so, you are breaking the law. The Data Protection of 1998 calls for all stored personal information to be relevant and up to date. Sort through those files and make sure you are in compliance with the law.

Data protection is everyone's job.

Frequently Asked Questions

1. What if the police or another department needs to see our files to prevent or detect crime?

2. Can I be held personally liable for a breach of the Code or Act?

3. Who should I go to if I have a query relating to the Act or if I think that someone may be using personal data incorrectly?

4. Who should have access to what data, bearing in mind the security requirements under the Act?

5. What is the meaning of "personal data"?

6. What does "fair" mean when the Act tells us data must be processed fairly and lawfully?

7. What if someone asks to see the information we hold about them?

Ten ways to help with data protection

- Lock up all paper files when going home for the day
- Password protect your computer when stepping out for lunch
- Shred documents containing personal data when disposing of them
- Don't take documents out of the office unless required
- When taking information from a client, don't record more data you need
- Record date of birth instead of age
- Keep personal information no longer then needed
- Don't distribute personal information needlessly around the council
- Remove excessive or out of date information from files
- Talk to your Data Protection Officer about any questions you may have.

Data Protection Act 1998

What you need to know...

Data Protection Officer
Simon Guild
x 4182
simon.guild@merton.gov.uk

merton
moving ahead

Principles of Data Protection

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. The definition of processing is far wider than before. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'.

Case Study

Breach: 1st and 2nd DPA Principles

In July of 2002 two employees at the 02 Mobile phone Company were convicted and fined for DPA offences. According to the court the two had violated the first and second principles of the act when they released text messages of a young women to her jealous boyfriend. Apparently the young women had been cheating on her boyfriend, who then convinced his two friends at O2 to forward the incriminating text messages to his account. In anger the boyfriend hacked into the women's Friends Reunited account and posted photographs of the two having sex. Then he sent e-mails to all her friends directing them to the sight. The boyfriend has since been jailed for five months, and the two O2 employees sacked. According to the Data Protection Act, the two broke the Fairly and lawfully process principle, as well as the processed for limited purposes principle. O2 itself, by not ensuring that the text message data was secure, may have violated the 7th principle.

Answers

1. The Act allows this under a section 29 exemption, provided it is strictly necessary for the prevention, detection of crime or the prosecution of offenders. Contact the Data Protection Officer and ask for advice.

2. It is possible, particularly if you were to disclose data or use it for non-council purposes, or if - as a manager - you become aware of a breach of the Act and take no action to remedy the position.

3. You should contact the Data Protection Officer and ask for advice.

4. The starting point is to limit access to the information strictly to those who 'need to know' as part of their duties. Who has what data should be known to key senior individuals so that if necessary data can be located and checked on short notice.

5. Personal data mean any information relating to an identified or identifiable living person ("data subject"). The processing of anonymous data, which does not identify persons, is not subject to data protection law.

6. Fair processing means that you are telling people what you are collecting their data for, who it may be disclosed to and any consequences of the processing the data subject is not aware of.

7. This is their right under the 1998 Data Protection Act. There are some restrictions so take their contact details and pass them to the Data Protection Officer.

Appendix S: Glossary of Terms

Computerised Data – Computerised data are any data held in a computer, or any data that is intended to be held on a computer that pertains to a living data subject. This includes E-mails, internet content, data bases, and word processing.

Data Controller – Data Controllers are the persons on whom most of the responsibility of the Data Protection Act of 1998 falls. It is their duty to determine the purpose for which and manner in which any personal data are, or are to be processed. A data controller must ensure that all the guidelines and regulations of the DPA 98 Act are followed by the data processors, and that the personal rights of data subjects are respected and followed.

Data Processor – A data processor will most likely be a person whom does data entry for a data controller. Whereas a data controller is in charge of overseeing correct procedure is followed for all personal data under his control, a data processor merely processes the data on behalf of the controller. The main distinction between a controller and a processor is that a processor only act on the instructions of the controller, and does not determine use data or purpose of processing.

Data Protection Commissioner – The current Data Protection Commissioner in the UK is Mr. Richard Thomas. It is his duty to promote good information handling and the encouragement of codes of practice for data and data controllers, as well as anyone who decides to process personal information.

Data Subject – A data subject is defined by the Act as "an individual who is the subject of personal data." The interpretation for this project of a data subject is any personal whose personal, private, and sensitive information is being stored and processed.

Processing – This particular word is intentionally left very vague by the Act. There are many attempts throughout the literature to narrow its meaning down as much as possible. The best explanation of processing as it is appears in the Act is doing *anything* to personal information. This such as changing, organizing, and transferring are just some examples of actions to personal data that fall under the term "processing" by the Act.

Personal Data – Personal data are defined by the Act in s. 1(1) as:

> Data which relate to a living individual who can be identified –
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the passion of, the data controller.

This is intended to describe that personal information is any information about a person that identifies that person, or could be rotationally used to identify that person. Almost any type of information about a person can be considered personal information.

Sensitive Data – Data that is concerned "sensitive" includes the following types of information

(a) Race/Ethnicity
(b) Political Opinions/Affiliations

(c) Religion Affiliations
(d) Trade Union Membership
(e) Health
(f) Sex Life
(g) Criminal Convictions, as well as allegations

Sensitive data requires the explicit permission of the data subject in order to process. However, many of these types of information often fall under areas of Act exemption, for example judicial procedures. Therefore before sensitive data may be processed, the use of an exemption must be cleared by a data controller.