

Control of Information Mark Scheme

1. A company, which sells goods over the Internet, purchased a mailing list of email addresses in the year 2001.

- (a) Explain why it was of benefit to the company to purchase a list of email addresses. (2)
- (b) Explain a limitation to the company of using this list. (2)
- (c) The company has data of a personal nature that they wish to sell.
 - (i) Whose permission must they first obtain? (1)
 - (ii) Whom should they inform of their intentions? (1)

- a) Saves time or money (1) as company does not have to collect the data themselves (1)**
- b) Data no longer up to date/email addresses don't necessarily correspond to people/people change e-mail address/ people change ISP/ people change email provider (1) means people .evaporate. so mail shot would be wasted /data no longer has value (1)**
- c) i. The data subject (1)**
 - ii. The Information Commissioner (1)**

2. A college maintains an extensive database of its full-time students. The database contains personal data, the courses students attend, and higher education or employment applications.

- (a) Describe how the college might keep the personal data of the students up to date. (3)

(a) The College could send or hand out annual forms which should be filled in with the most up-to-date students' personal information required by the college. The list should include current courses which the students are studying and should remove (not delete) from the roll, any students who have moved on to higher education, left the college for another school/college, or left for employment.

- (b) The college wishes to sell the personal data to a local sports retailer. An agreement is to be written between the college and the retailer. Describe three issues, relating to the data, which should be included in this agreement. (3)

(b) Adequate, relevant and not excessive in relation to registered purpose. The sports retailer does not need course details, or higher education application details. Presumably the personal data would only be required for mail shots.

Held no longer than necessary for the registered purpose. The data should be removed from the sports retailers' records once the student has left the college.

Surrounded by proper security Secure measures to protect personal data of the employees should be in place. (Firewalls, Access Levels, File permissions, backup procedures should be in place and data corruption and loss of integrity, should be avoided.)

N.B. The college must have registered the fact that they are going to be selling the data on. They must get the data subjects' permission to pass their data on.

- 3(a) State five of the principles of the 1998 Data Protection Act. (5)

(a) Principles of Data Protection

Data must be . . .

1. Obtained and processed fairly and lawfully

2. *Held for a lawful purpose as described in the register*
3. *Adequate, relevant and not excessive in relation to registered purpose*
4. *Accurate and up-to-date*
5. *Held no longer than necessary for the registered purpose*
6. *Used only for the registered purpose*
7. *Accessible to the individual concerned*
8. *Surrounded by proper security*

(b) Describe three exemptions to the 1998 Data Protection Act.

(3)

(b) Exemptions - The Act does not apply to . . .

- *Payrolls, pensions, accounts*
- *Data held for backup purposes only*
- *Names and addresses used for distribution purposes*
- *Data for personal, family or recreational use (e.g. data held for a hobby)*
- *Clubs and societies (as long as no member objects)*
- *Data that must be made public by law (e.g. electoral roll)*
- *Those keeping data for statistical or research purposes have to register but data subjects to not have the right to access the data*
- *Data held for the collection of tax*
- *Data held for the prevention of crime*
- *Data held for national security purposes*
- *Data held by credit reference agencies is covered by the Consumer Credit Act 1974*

Partial exemption is granted to health professionals and social workers where it is believed that access to the data may be harmful to the subject.

Case Study

A Liberal Democrat MP is to try to use the Data Protection Act to get MI5 to reveal any files, which they hold on him. MI5 said:

"No member of the public is permitted to see any Security Service files, except for historical records which have been declassified and released by the Public Record Office."

"The Service only investigates individuals whose activities fall within its statutory remit under the Security Service Act".

"Confidentiality

4. When buying a new house through a large estate agency, customers are asked if they object to the data they are giving to the estate agent being passed on to other companies.

(a) Explain why the estate agent must ask this question.

(2)

(a) They are passing on personal details and so need the data subjects' permission to do so, a prerequisite of the Data Protection Act, which they might otherwise be breaking.

(b) State, with an example, what the estate agent could do with the customers' details if they give permission for them to be passed on.

(2)

(b) Sell them on to companies for money. Personal data is a valuable commodity. They could also use the data within their own organisation, particularly if they have a finance broker who gains financial reward from mortgage companies for suggesting use of their products.

5The personnel department of a large company keeps records on all the employees of the company. These records contain personal data and details of the employees' position, training and medical history. The company is registered on the Data Protection Register and has to abide by the principles of the 1988 Data Protection Act. Three of these principles are:

- "Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed";

Only acquire and maintain data which will focus around: personal data, position, training and medical history

- "Personal data shall be accurate and, where necessary, kept up to date";

The department could send or hand out annual forms which should be filled in with the most up-to-date personal information required. The data should be removed (not delete) when any employees leave the company.

- "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against the accidental loss of or destruction of, or damage to, to personal data".

Secure measures to protect personal data of the employees should be in place. (Firewalls, Access Levels, File permissions, backup procedures should be in place and data corruption and loss of integrity, should be avoided.)

(6)

For each of the principles stated above, describe what the company must do to comply with them.

Total Marks:

30