DATA PROTECTION FOR SECONDARY EDUCATION

Prepared by the Data Protection Office of Mauritius
October 2016

CONTENTS

1 INTRODUCTION

The Data Protection Office has developed this material for Secondary School Students.

The aim of the resource is to raise awareness in the field of data protection amongst young people. This guide will assist secondary school students to understand their fundamental right to privacy, the importance of taking control over their personal information, the other rights they have when their personal information is collected or used and also how they may access their personal information.

The Data Protection Office is a public office and the head of the office is known as the Data Protection Commissioner.

2 THE VISION OF THE DATA PROTECTION OFFICE

The vision of the Data Protection Office is:

- A society where data protection is understood and practiced by all.
- The right to privacy and data protection is primordial to the sanctity of any modern democracy.
- The adoption of clear procedures for the collection and use of personal data in a responsible, secure, fair and lawful manner, by all data controllers and data processors.

3 MISSION

The primary mission of the Data Protection Office is to safeguard the processing of your personal data in the present age of information and communication.

4 OBJECTIVES

Functions of the Data Protection Office:

The Commissioner -

(a) ensures compliance with the Data Protection Act and any regulations made under it;

(b) issues or approves codes of practice or guidelines for the purposes of the Data Protection Act;

(c) creates and maintains a register of all data controllers and data processors;

(d) exercises control on all data processing activities, either of its own motion or at the request of a data subject, and verifies whether the processing of data is in accordance with the Data Protection Act or regulations made under the Act;

(e) promotes self-regulation among data controllers and data processors;

(f) investigates any complaint or information which gives rise to a suspicion that an offence under the Data Protection Act may have been, is being or is about to be committed;

(g) takes such measures as may be necessary so as to bring to the knowledge of the general public the provisions of the Data Protection Act;

(h) undertakes research into and monitor developments in data processing and computer technology, including data matching and data linkage and ensures that there are no significant risks of any adverse effects of these developments on the privacy of individuals;

(i) examines any proposal for data matching or data linkage that may involve an interference with, or may otherwise have adverse effects on the privacy of individuals and, ensure that any adverse effects of such proposal on the privacy of individuals are minimised;

(j) co-operates with supervisory authorities of other countries, to the extent necessary for the performance of her duties under the Data Protection Act, in particular by exchanging relevant information in accordance with any other enactment;

(k) does anything incidental or conductive to the attainment of the objects of, and to the better performance of her duties and functions under the Data Protection Act.

OBLIGATIONS UNDER THE DATA PROTECTION ACT

As more and more personal data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting legal responsibilities has increased.

Ignorance of the Data Protection Act leads to a great risk that personal data entrusted to Data Controllers will be retained, used and/or disclosed in ways that may breach individuals' data protection rights.

THE ROLE OF THE DATA PROTECTION OFFICE

1. The role of the Data Protection Office is to ensure that clear procedures on collection and use of personal data are adopted in a responsible, secure, fair and lawful manner with a view to protect personal data.
2. The Data Protection Office is committed to provide the best possible service to help organisations and the public at large to understand their data protection rights and obligations.
3. The Data Protection Office is playing a vital role since:
   a) Data protection is becoming fundamental to peoples' lives and for the good business reputations of public/ private organisations.
   b) Data protection reinforces modern democracy and the fundamental liberties entrenched in our constitution.
   c) Data protection is also essential to create and maintain a trusted relationship between the state and the citizen.
   d) Personal information, especially sensitive personal data which is the greatest asset of an organisation can also become the most dangerous liability, if it is not handled properly.

e) Information management demands clear lines of accountability and responsibility, coherent policies and procedures and rigorous training on data sharing.

f) The privacy of personal information has become a global responsibility for governments, commerce and civil society.

g) To preserve the wide-spread adoption and use of new technologies, we must build trust by promoting and ensuring the privacy of our personal information.

A SUMMARY OF THE KEY PARTS OF THE DATA PROTECTION ACT

1. The Data Protection Act has been updated to secure better chances of accreditation with the European Union for Mauritius to be recognised as an adequate country in data protection to facilitate the transfers of personal data from the European Union to Mauritius and thus attract more investment in mainly the information technology and business processing outsourcing sectors of the economy.
2. The Data Protection Act more importantly gives individuals the rights to protect them against data protection breaches, and creates obligations for those data controllers and processors who keep personal information.
3. The Data Protection Act also deals with the obligation for registration by Data Controllers and Processors.
4. It also concerns the right to access personal data of data subjects controlled/processed by data controllers/processors.
5. Under the Data Protection Act, individuals have the right to be informed of any data processing activity which relate to them as data subjects.
6. Investigations, audits and security checks are carried out by this office to assess compliance with the Data Protection Act.

THE DATA SUBJECT

A “data subject” is a living individual who is the subject of personal data.

Example of data subject:
A **student** or a **teacher** or a **director** or a **supplier** or **creditor/ debtor** is a “**data subject**” of the **XYZ Secondary School**.

7.2 WHAT IS DATA?

"**Data**" means information in a form which -

(a) (i) is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and

(ii) is recorded with the intent of it being processed by such equipment; or

(b) is recorded as part of a relevant filing system or intended to be part of a relevant filing system;

Example of data:

The data records held by the **XYZ Secondary School** can be categorised into:

(i) **Employee data** and

(ii) **Non-Employee data** such as shareholders, creditors, debtors, suppliers, students, etc.

7.3 WHAT IS PERSONAL DATA?

Personal data is defined as "data which relate to an individual who can be identified from those data; or data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion."

Examples of personal data:

(1) The personal data records of an employee held by the XYZ Secondary School can be:

(a) Name, address, telephone number or email addresses & contact details,

(b) Date of birth, NIC number, Marital Status,

(c) Educational certificates or previous employment history,

(d) Original records of application and appointment,

(e) Interview records & references,

(f) Record of appointments to promotion posts,

(g) Details of approved absences such as sick leave, casual leave, etc,

(h) Records of any courses/trainings attended,

(i) Details of work experience,

(j) Details of complaints/weaknesses or competencies/ strengths,

(k) Pension compilation records,

(l) Salary, payroll details, bank details,

(m) Medical card details.

The purpose/s for the Data Controller to keep employees' data may be justified to:

- process payroll for staff,
- calculate pension payments in the future,
- process human resources management,
- compute recording promotions etc, and
- be compliant with local laws.

(2) The personal data records of a student held by the XYZ Secondary School can be:

(a) Name, address, telephone number or email addresses & contact details,

(b) Contact details such as telephone number or email addresses,

(c) Date of birth,

(d) NIC number,

(e) Names and addresses of parents/guardians and their contact details,

(f) Religious belief,

(g) Racial, ethnic or national origin,

(h) Information on previous academic records,

(i) Psychological assessments,

(j) Attendance records,

(k) Academic records – subjects studied, class assignments, examination results,

(l) Records of disciplinary issues and/or sanctions imposed,

(m) Other records e.g. records of any serious injuries/ accidents etc.

The purpose/s for the Data Controller to keep non-employees' (student) data may be justified to:

- monitor attendance records,
- process certificates, examinations, and
- be in compliance with local laws.

7.4

SENSITIVE PERSONAL DATA

Some groups of information are categorised as **sensitive personal data** under the Data Protection Act.

Sensitive Personal Data refers to personal information regarding a person's:

(a) racial or ethnic origin;

(b) political opinion or adherence;

(c) religious belief or other belief of a similar nature;

(d) membership to a trade union;

(e) physical or mental health;

(f) sexual preferences or practices;

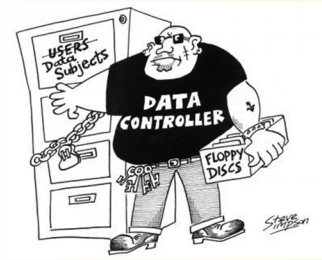
(g) commission or alleged commission of an offence; or

(h) proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Example of Sensitive Personal Data:

The **XYZ Secondary School** may hold some or all of the sensitive information about its employees such as medical information which consists of sickness absence and medical certificates.

The purpose for keeping this type of information is to process sick leave pay and disability entitlement, which will be used to monitor and manage sickness absence and to comply with health and safety obligations



7.5 DATA CONTROLLER

A **Data Controller** is "a person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be processed."

Example of a data controller:

The **XYZ Secondary School** is the **Data Controller**.

7.6 DATA PROCESSOR

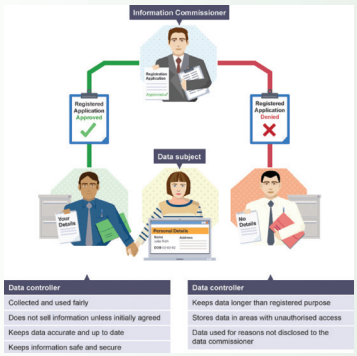
A **Data Processor** is "a person, other than an employee of the data controller, who processes the data on behalf of the data controller."

A data controller or a data processor may either be a public or a private institution.

The Data Protection Act will apply to a data controller:
(a) who is established in Mauritius; and
(b) who is not established in Mauritius, but uses equipment in Mauritius for processing data for other purposes than mere transit.

A data controller is deemed to be established when he is a resident in Mauritius and/or carries out data processing activities through an office, branch or agency in Mauritius. When not established in Mauritius, a data controller must nominate a representative in Mauritius.

The data protection agenda ranges from biometrics to simple personal details kept or processed in a structured filing system or on a computer such as names, addresses and identity numbers as it concerns all information directly or indirectly related to a living individual.



7.7 REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

The principal purpose for registration is legal compliance. The creation of a public register by the Data Protection Office is to meet transparency and openness. The public has a need to know or should be able to find out which Data Controller/Data Processor has been registered with the Data Protection Office and is carrying out processing of the personal data. The Data Protection Office must also know the purposes for which the Data Controller and Data Processor are keeping or processing the personal data to carry out the business. If a Data Controller/ Processor discloses false information to the Data Protection Office, he may be prosecuted.

THE DATA PROTECTION ACT (SECTION 33)

Section 33 of the Data Protection Act provides that every data controller and data processor must before keeping or processing personal data or sensitive personal data, register himself with the Data Protection Office upon the payment of the relevant fees enacted under the Data Protection Regulations.

Failure to register or to renew registration within three months before the date of expiry of registration, on an annual basis, is an offence under the Act and the regulations.

7.8

SECURITY AT THE HEART OF THE DATA PROTECTION ACT

1. A data controller shall –
   (a) take appropriate security and organisational measures for the prevention of unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of the data in his control; and
   (b) ensure that the measures provide a level of security appropriate to –
      (i) the harm that might result from the unauthorised access to, alteration of, disclosure of, destruction of the data and its accidental loss; and
      (ii) the nature of the data concerned.
2. A data controller or a data processor shall take all reasonable steps to ensure that any person employed by him is aware of and complies with the relevant security measures.
3. Where a data controller is using the services of a data processor, he shall choose a data processor providing sufficient guarantees in respect of security and organisational measures for the purposes of complying with subsection.

Example of Security:

The school acknowledges that high standards of security are essential for keeping and processing of all personal information and a copy of the database is kept far away to a remote secured place for any disaster recovery.

8

THE DATA PROTECTION PRINCIPLES

The data protection principles represent the main milestones of data protection law which need to be vigilantly followed and exactly implemented by all sectors.

Briefly, they are the good practices to be executed by all.

8.1 THE 8 DATA PROTECTION PRINCIPLES

They are as follows:

1. **Principle of lawfulness and fairness.**
   Personal data shall be processed fairly and lawfully.
2. **Principle of purpose specification**
   Personal data shall be obtained only for any specified and lawful purpose/s, and shall not be further processed in any manner incompatible with that/these purpose/s.
3. **Principle of adequacy and relevance**
   Personal data shall be adequate, relevant and not excessive in relation to the purpose/s for which they are processed.
4. **Principle of accuracy**
   Personal data shall be accurate and, where necessary, kept up to date.
5. **Principle of time limitation**
   Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.
6. **Principle of respect for privacy rights**
   Personal data shall be processed in accordance with the rights of the data subjects under the Data Protection Act.
7. **Principle of security**
   Appropriate security and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. **Principle of control over transborder data flows**
   Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

8.2 APPLYING DATA PROTECTION PRINCIPLES:

Example:

The Data Protection Act deals with rights on individuals as well as responsibilities on those persons controlling and processing personal data. The **XYZ Secondary School** keeps personal data of individuals on computer or in structured manual files.

1. **Principle of lawfulness and fairness**

   The **XYZ Secondary School** must ensure that data subjects (staff, students & parents) are aware of the following for the lawful collection of personal data:

   - the name of the school (the “data controller”);
   - the persons or categories of persons to whom the data may be disclosed;
   - the existence of the right of access to their personal data;

2. Principle of purpose specification

The **XYZ Secondary School** must ensure that data subjects (staff, students & parents) are aware of the purpose/s of collecting and processing any personal data.

3. Principle of adequacy and relevance

The personal data held by **XYZ Secondary School** must be adequate, relevant and not excessive in relation to the purpose/s for which it is kept.
Periodic processing of files must show that personal data held is not excessive and remains adequate and relevant for the purpose for which it is kept.

4. Principle of accuracy

The **XYZ Secondary School** must establish procedures to ensure that personal data are accurate and complete.

The **XYZ Secondary School** relies on the individuals who supply personal data (staff, students and others) to ensure that correct and up-to-date personal information are provided.

Any changes brought to the personal information must be communicated to **XYZ Secondary School**.

5. Principle of time limitation

The **XYZ Secondary School** must have a defined policy on retention periods for personal data and appropriate procedures.

In the setting up of retention periods for different groups of data, the following issues have been considered:

(i) the relevant legislative requirements,

(ii) the possibility of litigation,

(iii) the retention periods laid down by finance authorities and

(iv) the requirement to keep an archive for historical purposes.

The school whilst registering books for students may require data to be kept and archived indefinitely within the school in order to provide testimonials to any students on request at any time.

The salary, taxation and related employment records are to be retained in accordance with the time periods set out within the established laws.

Where litigation may arise in the future (e.g. in relation to accidents/ personal injuries involving employees/students or accidents occurring on school property), the relevant records need to be retained until the possibility of litigation ceases.

6. Principle of respect for privacy rights

The **XYZ Secondary School** must only use and disclose personal data in ways that are necessary for the purpose/s or compatible with the purpose/s for which the data has been collected as per the Data Protection Act.

The **XYZ Secondary School** must ensure that staff/department involved in processing personal data are aware of the purpose/s of collecting such data and use/process it only for that specific purpose or compatible purpose/s.

7. Principle of security

The **XYZ Secondary School** stores all personal information in a centralised controlled access database (including computerised and manual files) at the rector's office.

The school must take all the appropriate security measures against any unauthorised access to, or alteration, disclosure or destruction or accidental loss of the data. Access to files containing personal data (computerised and manual) must be restricted to only the authorised staff who works in that particular field.

Computer systems are password protected and are backed up daily to a secured server.

The offices are secured and alarmed (monitored) when not occupied.

Waste paper which includes personal information is confidentially shredded before it is disposed as waste.

8. Principle of control over transborder data flows

To send any data abroad, a request must be sent to the Data Protection Commissioner for necessary authorisation.

The country of destination, the period of data transfer and the purpose/s for sending any personal data abroad must be clearly mentioned to seek authorisation from the Data Protection Office.

After authorisation is granted, all modes of transfer must be done in a secured channel in order to prevent any hacker/cracker to intercept the personal information which is in transit.

The personal data which have already been sent abroad, are then regulated by the Data Protection Authority of the destination country, if any.

If the country of destination does not have any data protection laws, then the data controller of the destination country must provide the guarantee that all the data will be protected and secured.

RIGHTS OF DATA SUBJECTS

Under section 41 of the Act, a data controller must upon the written request of a data subject inform the data subject on

a. any personal data kept by him (data controller);
b. the purpose/s for keeping the data; and
c. the third parties to whom the data may be disclosed by the data controller.

A data controller may refuse to comply with the request if he is not provided with such information as he may reasonably require to determine the identity of the data subject and to locate the information being requested.

EXEMPTIONS UNDER THE DATA PROTECTION ACT

There is no exemption from registration catered for in the law, except for:

- personal data which is required for national security purposes; and
- personal data processed by an individual strictly for personal, family, household or recreational purposes.

Other fields that are exempted only from certain varying sections or all of the sections of the Data Protection Act, are for:

i national security,
ii. crime and taxation,
iii. health and social work,
iv. regulatory activities,
v. journalism, literature, art, research, history and statistics,
vi. information available to the public under an enactment,
vii. disclosure required by the law or in connection with legal proceedings,
viii. legal professional privilege, and
ix. domestic purposes.

Data controllers should further exercise caution when relying upon an exemption under the Act and should not regard it as providing automatic or blanket exclusion from the application of the provisions of the Act.

QUESTIONS

1. What is the vision of the data protection office?
2. What is the primary mission of the data protection office?
3. Give 5 functions of the Data Protection Commissioner?
4. Who is a data subject?
5. What do you understand by the term ‘data’ in the context of the data protection?
6. Define ‘personal data’?
7. What does ‘Sensitive Personal Data’ refer to?
8. Who is a Data Controller?
9. What do you understand by ‘Data Processor’?
10. Why the Data Controller needs to be registered to the Data Protection office?
11. Why a data controller must take appropriate security and organisational measures for all personal data which is in his control?

CASE STUDIES

(a) Case Study 1 - Closed-circuit television (CCTV)

Closed-circuit television (CCTV) which is also known as **video surveillance**, is the use of video cameras to transmit the recorded images to a specific place, on a limited set of monitors. CCTV systems have been installed in the **ABC Secondary School** within the perimeter walls/fencing and inside the school. These CCTV systems record images of staff, students and members of the public who visit the premises.

CCTV systems safeguard school property, equipment as well as safety and security of staff, students and visitors.

All the angles of the cameras of are focused and fixed permanently within the parameters of the school which can only capture images within the premises of the school ensuring that no personal data are recorded outside the walls/fencing.

The recording equipment is located in the Principal's Office. Access to images/ recordings is strictly restricted to the Principal & Deputy Principal of the school. Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident.

Questions on Case Study 1

(a) Who is the data controller?
(b) Identify all the data subjects of the ABC Secondary School.
(c) What is the purpose of installing the CCTV camera at ABC Secondary School?
(d) How to ensure that no images are being recorded outside the parameters of ABC Secondary School by CCTV cameras?
(e) Describe the security issues of the personal data being captured at ABC Secondary School?
(f) Find the retention period of the personal data of the CCTV kept at ABC Secondary School?
(g) Identify how consent can be obtained to capture the images of the data subjects?

(b) Case Study 2- Unsolicited text message

To promote the sales of pizza, **ABC Pizza Group** sends mass sms to a group of people.

In city XYZ, many individuals started receiving unsolicited text messages on their private mobile phones sent by ABC Pizza Group without their consent and without the inclusion of an opt-out facility.

Most of the time, complainants continued to receive unsolicited marketing text messages after placing orders in different ABC Pizza Group stores.

Many individuals complained to ABC Pizza Group to stop sending them such type of text messages. Despite these complaints, ABC Pizza Group continued to send text messages on their mobile phones.

Questions on Case Study 2

(a) Are mobile phone numbers personal data?

(b) What is an 'unsolicited' message?

(c) Is consent of an individual required to send him/her telemarketing messages?

(d) What is an 'opt-out' facility?

(e) Can the individual make a formal complaint against ABC Pizza Group to the Data Protection Office?

(f) What corrective measures can be taken by ABC Pizza Group to address this situation?

(c) Case Study 3- Disclosure of students' Personal Data

SS School keeps personal data of students in its database. The parent of Jenny has requested the personal details regarding Mary from the school. The **SS School** has disclosed the personal details of Mary to the parent of Jenny. Mary has complained to the Data Protection Commissioner on this unlawful disclosure to the detriment of Mary. The letter from the school was addressed "To Whom It May Concern" where the personal details of the Mary were disclosed to Jenny's parent and the latter has used the letter to the detriment of Mary at another school.

Questions on Case Study 3

(a) Who is the data controller? Why?

(b) Who is the Data Subject whose details were disclosed?

(c) What possible offence was committed? By whom?

(d) What actions can be taken by the Data Protection Commissioner?

ANSWERS TO QUESTIONS

1. The vision of the Data Protection Office is:

- A society where data protection is understood and practiced by all.
- The right to privacy and data protection is primordial to the sanctity of any modern democracy.
- The adoption of clear procedures for the collection and use of personal data in a responsible, secure, fair and lawful manner, by all data controllers and data processors.

2. The Mission of the Data Protection Office is:

The primary mission of the Data Protection Office is to safeguard the processing of your personal data in the present age of information and communication

3. Choose any 5 functions of the Data Protection Commissioner from the list below:

The Commissioner -

(a) ensures compliance with the Data Protection Act, and any regulations made under it;

(b) issues or approves codes of practice or guidelines for the purposes of the Data Protection Act;

(c) creates and maintains a register of all data controllers and data processors;

(d) exercises control on all data processing activities, either of its own motion or at the request of a data subject, and verifies whether the processing of data is in accordance with the Data Protection Act or regulations made under the Data Protection Act;

(e) promotes self-regulation among data controllers and data processors;

(f) investigates any complaint or information which gives rise to a suspicion that an offence under the Data Protection Act may have been, is being or is about to be committed;

(g) takes such measures as may be necessary so as to bring to the knowledge of the general public the provisions of the Data Protection Act;

(h) undertakes research into and monitor developments in data processing and computer technology, including data-matching and data linkage and ensures that there are no significant risks of any adverse effects of these developments on the privacy of individuals;

(i) examines any proposal for data matching or data linkage that may involve an interference with, or may otherwise have adverse effects on the privacy of individuals and, ensure that any adverse effects of such proposal on the privacy of individuals are minimised;

(j) co-operates with supervisory authorities of other countries, to the extent necessary for the performance of her duties under the Data Protection Act, in particular by exchanging relevant information in accordance with any other enactment;

(k) does anything incidental or conducive to the attainment of the objects of, and to the better performance of her duties and functions under the Data Protection Act.

4. A "**data** subject" is a living individual who is the subject of personal **data**.

   For Example:

   A **student** or a **teacher** or a **director** or a **supplier** or **creditor**/ **debtor** is a "**data subject**" of the **XYZ Secondary School**.

5. "**Data**" means any information in a form which -

   (a) (i) is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and

   (ii) is recorded with the intent of it being processed by such equipment; or

   (b) is recorded as part of a relevant filing system or intended to be part of a relevant filing system;

   Example of data:

   The **Data** records held by the **XYZ Secondary School** can be categorised into:

   (j) **Employee data** and

   (ii) **Non-Employee data** such as shareholders, creditors/debtors, suppliers, students, etc.

6. Personal data is defined as "data which relate to an individual who can be identified from those data; or data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion."

7. **Sensitive Personal Data** refers to personal information regarding a person's:

   (a) racial or ethnic origin;

   (b) political opinion or adherence;

   (c) religious belief or other belief of a similar nature;

   (d) membership to a trade union;

   (e) physical or mental health;

   (f) sexual preferences or practices;

   (g) commission or alleged commission of an offence; or

   (h) proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;

8. A **Data Controller** is "a person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be processed."

9. A **Data Processor** is "a person, other than an employee of the data controller, who processes the data on behalf of the data controller."

10. The principal purposes for registration are legal compliance and transparency.

11. A data controller must take appropriate security and organisational measures for all personal data he is keeping in order to prevent unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of the data in his control.

ANSWERS TO CASE STUDIES

Case Study 1 Answer on CCTV

(a) ABC Secondary School is the Data Controller.

(b) The data subjects are staff, students and members of the public who visit the premises.

(c) The purpose of installing the CCTV systems are to safeguard school property, equipment as well as safety and security of staff, students and visitors.

(d) All cameras are focused and permanently fixed within the parameters of the school only to capture images within the premises of the school ensuring that no personal data are recorded outside the walls/fencing.

(e) Access to images/recordings is restricted to the Principal & Deputy Principal of the school. The data are kept in tapes, DVDs, hard disk recordings for 28 days, except if required for the investigation of an incident.

(f) The retention period is 28 days, except if required for the investigation of an incident.

(g) This will be achieved by adopting appropriate data protection notices at the point of data capture e.g. A visible sign noticed placed at the gate before entrance, “Area under camera surveillance” so that the data subject will be aware that they are entering premises which are under camera surveillance. Staff Application forms and student enrolment forms can be used where an express signature of indication of consent is not necessarily always required.

Case Study 2 Answer - Unsolicited text message

(a) Yes. A mobile phone number is registered to a user and can thus identify him/her.

(b) An unsolicited message means a message which has not been requested or asked for.

(c) Yes.

(d) An opt-out message is a message which includes an easy option for the recipient to be removed from any future messages.

(e) Yes.

(f) ABC Pizza Group has to ensure that a proper mechanism is put into place to record consent of individuals and ensure that telemarketing messages are sent to only those individuals who have provided their express consent to receive them.

(g) ABC Pizza Group must ensure that an opt-out facilities are provided to people who no longer wish to receive such text messages.

Case Study 3 Answer - Disclosure of a student Personal Data

(a) SS school is the data controller because it keeps the personal data of students.

(b) Mary is the data subject.

(c) The offence committed by the SS school was an unlawful disclosure of Mary's personal data to Jenny's parent who disclosed it further to another school without the consent of Mary.

(d) If complaint will be lodged to the Data Protection Office, the Data Protection Commissioner will investigate into the matter and will refer the case to the relevant authority (Police Department) for prosecution regarding the unlawful disclosure of personal data after conducting an inquiry with the school.