

CHAPTER 5: DATA PROTECTION

The Data Protection Act contains 8 Principles. These state that all data must be:

- Processed fairly and lawfully
- Obtained & used only for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate, and where necessary, kept up to date
- Kept for no longer than necessary
- Processed in accordance with the individuals rights (as defined)
- Kept secure
- Transferred only to countries that offer adequate data protection

The legislation underpinning these principles is complex and not really suitable for direct devolution to all the staff who may have responsibility for personal data. Nor does it provide a measure of compliance. Hence the need for supporting products and information

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data.

Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data privacy issues are:

- Health information
- Criminal justice
- Financial information
- Genetic information
- Location information

The challenge in data privacy is to share data while protecting personally identifiable information. Consider the example of health data which are collected from hospitals in a district; it is standard practice to share this only in the aggregate. The idea of sharing the data in the aggregate is to ensure that only non-identifiable data are shared.

The legal protection of the right to privacy in general and of **data privacy** in particular varies greatly around the world.

Ten rules of data protection

1. Consent

Wherever possible obtain consent before acquiring, holding or using personal data. Any Staffordshire University forms, whether paper or web-based, which are designed to gather personal data should contain a statement explaining what the information is to be used for and who it may be disclosed to.

2. Sensitive data

Be particularly careful with sensitive personal data (i.e. information relating to race, political opinion, physical or mental health, religious belief, trade union membership, sexuality, criminal offences etc). Such information should only be held and used where strictly necessary. Always obtain the consent of the individual concerned and notify them of their likely use(s) of such data.

3. Individual rights

Wherever possible be open with individuals concerning the information being held about them. When preparing reports or appending notes to official documents, bear in mind that individuals have the right to see all personal data and could therefore read any 'informal' comments made about them. Also be aware that this includes e-mails containing personal data and so the same caution should be used when sending e-mails.

4. Review files

Only create and retain personal data where absolutely necessary. Securely dispose of or delete any personal data which is out of date, irrelevant or no longer required. Hold regular reviews of files and discard unnecessary or obsolete data systematically.

5. Disposal of records

When discarding paper records that contain personal data treat them confidentially (i.e. shred such files rather than disposing of them as waste paper). Similarly any unnecessary or out-of-date electronic records should be deleted. University computers should not be given away or sold unless Information Services have ensured that all information stored on it has been removed or deleted.

6. Accuracy

Keep all personal data up to date and accurate. Note any changes of address and other amendments. If there is any doubt about the accuracy of personal data then it should not be used.

7. Security

Keep all personal data as securely as possible (e.g. in lockable filing cabinets or in rooms that can be locked when unoccupied). Do not leave records containing personal data unattended in offices or areas accessible to the members of the public. Ensure that personal data is not displayed on computers screens visible to passers-by. Be aware that these security considerations also apply to records taken away from the University e.g. for work at home or for an external meeting. Also bear in mind that e-mail is not necessarily confidential or secure so should not be used for potentially sensitive communications.

8. Disclosing data

Never reveal personal data to third parties without the consent of the individual concerned or other reasonable justification. This includes parents, guardians, relatives and friends of the data subject who have no right to access information without the data subject's consent. Personal data can only be legitimately disclosed to third parties for purposes connected with a student's studies and to meet statutory requirements (e.g. to HEFCE, LEAs, Council Tax Offices and Research Councils) but only where we are satisfied to the enquirers' identity and the legitimacy of the request.

Requests for personal information are received from time to time from organisations such as the police and the inland revenue. The University endeavours to co-operate with these organisations but steps should first be taken to ensure that requests are genuine and legitimate.

9. Worldwide transfer

Always obtain consent from the individual's concerned before placing information about them on the Internet (apart from basic office contact details) and before sending any personal data outside the European Union, Iceland, Lichtenstein or Norway.

10. Third party processors

Be aware that if you are using a third party data processor e.g. for bulk mailings or database management and are giving them access to personal data, then you must have a written contract in place with them to ensure that they treat such information confidentially, securely and in compliance with the Data Protection Act 1998.

Data Protection Act (DPA) Compliance

The Data Protection Act was implemented in 1998 with the purpose of safeguarding the fundamental rights of individuals with regard to the processing of personal data and the free movement of such data.

To achieve compliance with the Data Protection Act, organizations and government bodies must adhere to its principles that deal with the processing of personal data.

Sanctuary Helps Organizations and Government Bodies Comply with the Data Protection Act for Endpoint Security

SecureWave Sanctuary ensures privacy of personal data by enforcing encryption when copied to removable media. Sanctuary also provides detailed audit information to prove compliance with the DPA's principles. With Sanctuary, only authorized users can copy personal data onto encrypted removable media with complete auditing of that action.

By employing a whitelist approach, Sanctuary is uniquely capable of enforcing application and device usage and control policies, which enables only authorized applications and devices to run or connect to a network, server, terminal services server, laptop, thin client or desktop – facilitating security and systems management, while providing necessary flexibility to the organization to easily enable the use of new/upgraded applications or devices.

Through policy-based control at the endpoints to monitor and control the inbound and outbound flow of personal data to media and devices, Sanctuary complements organizations' Data Protection Act compliance strategy by implementing measures to protect unauthorized transfer of personal data:

<u>Data Protection Act Principle</u>	<u>How Sanctuary Addresses Data Protection Principles</u>
<p>Principle 1 Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless-</p> <p>(a) at least one of the conditions in Schedule 2 is met</p> <p>(b) in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met.</p>	<p>Sanctuary enforces policies that control device and application use to prevent unauthorized processing of data. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC.</p> <p>Granular permissions enable policies to be enforced by user, user group, machine, time constraints, encryption, volume of data, data transfer and more criteria. Sanctuary also controls the types of files that are moved to and from removable</p>

	<p>devices to reduce the risk of unwanted files from entering the network and sensitive files from leaving the network. For further control, separate policies can be defined when the user is online or offline.</p> <p>This capability of granular policy enforcement significantly reduces the risk of unauthorized disclosure of sensitive data. Furthermore, Sanctuary provides a detailed audit trail of all device and application execution attempts and tracks all data that is copied to and from removable devices.</p>
<p>Principle 2 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.</p>	<p>Sanctuary enforces policies that control device and application use to prevent unauthorized processing of data. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC.</p> <p>Granular permissions enable policies to be enforced by user, user group, machine, time constraints, encryption, volume of data, data transfer and more criteria. Sanctuary also controls the types of files that are moved to and from removable devices to reduce the risk of unwanted files from entering the network and sensitive files from leaving the network. For further control, separate policies can be defined when the user is online or offline.</p> <p>This capability of granular policy enforcement significantly reduces the risk of unauthorized disclosure of sensitive data. Furthermore, Sanctuary provides a detailed audit trail of all device and application execution attempts and tracks all data that is copied to and from removable devices.</p> <p>With Sanctuary, organizations can monitoring all device and application execution attempts as well as monitor the amount of data and file types that are copied to and from removable devices.</p>
<p>Principle 3</p>	<p>Sanctuary controls the types of files that</p>

<p>Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.</p>	<p>are moved to and from removable devices to reduce the risk of unwanted files with personal data from entering the network and sensitive files from leaving the network. File size restrictions can also be enforced.</p>
<p>Principle 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.</p>	<p>Sanctuary ensures that personal data shall be processed in accordance with rights of data subjects by enforcing policies that control device and application use to prevent unauthorized processing of personal data. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a desktop, laptop, server, terminal services server or thin client.</p> <p>Sanctuary's granular permissions enable policies to be enforced by user, user group, machine, time constraints, encryption, volume of data, data transfer and more criteria:</p> <ul style="list-style-type: none"> • Restrict the daily amount of data that is copied from an endpoint to a device on a per-user basis • Block the PS/2 port, enforce the usage of USB keyboards and detect/block popular models of USB keyloggers to reduce the risk of attackers from capturing passwords and other confidential information through keyloggers • Record data that is read from and/or written to a removable device so that an organization reduces the risk of data leakage • Control the types of files that are moved to and from removable devices to reduce the risk of unwanted files from entering the network and sensitive files from leaving the network

	<p>For further control, separate policies can be defined when the user is online or offline, and permissions can be set temporarily or on a scheduled basis.</p>
<p>Principle 7 Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.</p>	<p>Sanctuary ensures appropriate technical and organizational measures by enforcing policies that control device and application use to prevent unauthorized processing of data. By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a desktop, laptop, server, terminal services server or thin client.</p> <p>Sanctuary's granular permissions enable policies to be enforced by user, user group, machine, time constraints, encryption, volume of data, data transfer and more criteria:</p> <ul style="list-style-type: none"> • Restrict the daily amount of data that is copied from an endpoint to a device on a per-user basis • Block the PS/2 port, enforce the usage of USB keyboards and detect/block popular models of USB keyloggers to reduce the risk of attackers from capturing passwords and other confidential information through keyloggers • Record data that is read from and/or written to a removable device so that an organization reduces the risk of data leakage • Control the types of files that are moved to and from removable devices to reduce the risk of unwanted files from entering the network and sensitive files from leaving the network <p>For further control, separate policies can be defined when the user is online or offline, and permissions can be set temporarily or</p>

	on a scheduled basis.
<p>Principle 8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.</p>	<p>Sanctuary ensures adequate level of protection by centrally encrypting removable media or forcing end users to encrypt media at the time of use, reducing the risk of personal data from being exposed to those without authorized access. Sanctuary can also control the type of files that are moved to and from removable devices, reducing the risk of personal data from being transferred outside of the network. Furthermore, Sanctuary's detailed auditing capabilities can be used to show what users and devices accessed or attempted to access sensitive information.</p>

Learning Outcomes

- Students should be able to define data protection and data privacy
- Students should be able to be data protection act compliance

Basic Reading

1. Greenstin, Marylyn. (2002). Electronic commerce; security, risk management, and control. 2nd Ed. Boston

Revision Questions

1. Differentiate between data protection and data privacy.
2. Identify and explain the TEN rules of data protection.