Data Protection in the Digital Age: Implications for Higher Education Institutions

WHY MUST WE PROTECT PERSONAL DATA

- It is a legal requirement
- It enhances quality education
- It aims to improve consumer protection and general levels of privacy for individuals,
- Promotes good information handling practices
- Protects University reputation
- Individually are increasingly aware their data rights
- Fines if you get it wrong

DATA PROTECTION LEGISLATION

- Xeerka Dhawrista Xogta Dadweynaha, Dawlada Fadaralka Somalia
- Xeerka ilaalinta Xogta, Somaliland
- General Data Protection regulation (GDPR)

WHAT IS PERSONAL DATA

- Personal Data is any information relating to a natural Person
- For example, Registry student records, HR documents related to staff, payroll office records

WHAT IS 'SPECIAL' OR 'SENSITIVE' DATA?

- A category of data which must not be processed unless allowed for under certain specific exemptions, most usually where explicit consent is obtained. It refers to a person's:

–Race / ethnicity

–Political opinions

–Religious or philosophical beliefs

–Trade union membership

–Health data

–Sexual Life / Health / Orientation

SCOPE OF THE DATA PROTECTION

Any / all information relating to an individual e.g.

- Information held in manual form or printed out
- Emails, databases, spreadsheets etc.
- Photographs on web sites, marketing photographs, ID Cards
- CCTV images, Web pages
- Information which may be associated with online,etc

WHAT IS 'PROCESSING'

- Processing means performing any operation on personal data, whether or not by automated means, including:
- Collecting, recording, Organising, Storage, Altering, Disclosing, transferring and destruction

LEGITIMATE GROUNDS FOR PROCESSING PERSONAL DATA

- **Necessary for the performance of a contract with the data subject, or to take steps to prepare for a contract.**

LEGITIMATE GROUNDS FOR PROCESSING PERSONAL DATA

- **Necessary for compliance with a legal obligation**
- For example the University would need to process data e.g. to check an employee's entitlement to work , to deduct tax or to comply with health and safety laws.

LEGITIMATE GROUNDS FOR PROCESSING PERSONAL DATA/SPECIAL DATA

- **Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent**
- e.g. for medical emergencies. A ground for processing necessary for humanitarian purposes as well (e.g. disaster responses).

LEGITIMATE GROUNDS FOR PROCESSING PERSONAL DATA

- Necessary for the performance of a task carried out in the public interest or as a consequence of an official authority vested in the institution ("the public task")
- Necessary for the purposes of legitimate interests pursued by the University

LEGITIMATE GROUNDS FOR PROCESSING PERSONAL DATA/SPECIAL DATA

Consent

- Consent is only one of the legitimate grounds for processing personal data and special data . It should only be used where an individual is offered a genuine choice to either accept or decline what is being offered without suffering any detriment. e.g. access to free wifi only if the user consents to receiving marketing materials would be unacceptable as the two things are unrelated.

LEGITIMATE GROUNDS FOR PROCESSING PERSONAL DATA/SPECIAL DATA

- Data made public by the data subject
- Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

LEGITIMATE GROUNDS FOR PROCESSING PERSONAL DATA/SPECIAL DATA

- Necessary for reasons of substantial public interest
- Necessary for the purposes of the provision of health or social care or treatment or management of health or social care
- Necessary for archiving purposes in scientific and historical research purposes or statistical purposes

DATA PROTECTION PRINCIPLES

- **Data processed lawfully, fairly and in a transparent manner**
  - Lawfulness
  - Fairness
  - Transparency

DATA PROTECTION PRINCIPLES

- **Data obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**
  - **Purpose Limitation**

Decide what your basis is for collecting the personal information / special categories information and make this known to the individuals concerned e.g. on your website, in any literature.

DATA PROTECTION PRINCIPLES

- **Data processed is adequate, relevant and limited to what is necessary**

Data minimisation

Only collect and use what you actually need in order to carry out the purpose, and importantly, only what is compatible with the reasons and purposes which the individuals were informed of, or the purposes for which you are legally entitled to hold the information

DATA PROTECTION PRINCIPLES

- **Data is accurate and, where necessary, kept up to date**

Accuracy

Make sure that any personal data, or special categories data, collected is recorded accurately.
Every reasonable step must be taken to ensure that any data found to be inaccurate is erased or rectified without delay, and in any event within a month of receiving a request from the individual.

DATA PROTECTION PRINCIPLES

- **Data should not to be kept longer than is necessary for the purpose**

Storage Limitation

We cannot hold data any longer than is necessary for the purpose notified to the individual in our privacy notice / data collection notice etc.

DATA PROTECTION PRINCIPLES

- Appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction ,
- integrity and confidentiality

Information Security

- **Never disclose your password**
- Ensure your password is strong and change it regularly
- Always log off, or lock a workstation before leaving it
- When working on confidential work and / or on work involving personal data make sure no one else can read your screen
- Protect equipment from physical theft (especially laptops and memory sticks)

Electronic records and Database Systems

- Protect equipment from physical theft (especially laptops and memory sticks)
- Store all data on the University network so that it is backed up regularly
- Remember to back up and secure work mobile devices (laptop / phone) as well
- When sending emails internally or externally it is essential to check that the appropriate recipient has been selected, before sending the message
- Be careful with attachments – check they are the right ones before pressing “send”.

ACCOUNTABILITY

The University is responsible for and should be able to demonstrate compliance with the six principles.

What does this mean in practice?

1. Adherence to approved policies
2. Assign staff responsible for data protection
3. Good records management is essential.
4. Staff Training – ensure all staff know about data protection legislation and encourage attendance
5. Audits of compliance though internal / external auditors
6. Regular reports to the Compliance Task Group

INDIVIDUAL RIGHTS

- The right to be informed (privacy notice / data collection notice)
- The right of access (subject access request)
- The right to rectification (if data is inaccurate or incomplete)
- The right to erasure (previously known as the right to be forgotten)

- The right to restrict processing
- The right to data portability, The right of access
- The right to object