

CARETAKERS / ATTENDANTS / CLEANERS

DEFINITIONS OF AREAS WITHIN THE INSTITUTE

Secure Area: Any area which, in the normal course of business, would be locked when vacant.

Lecturing Area: Any area which is used for lecturing/teaching purposes and would, in the normal course of business, be locked when not in use.

Public Area: Any area which is accessible to the public when the Institute is open.

INSTRUCTIONS

Secure Areas: Ensure doors/windows are locked when exiting.

Public/lecturing areas – Where you suspect that electronic devices, e.g: phones, USB keys, or documents, have been left unattended for a period of time and may contain personal data, you should hand in to the Admin office in the Faculty or to the Information and Compliance Officer

DON'TS

- ⇒ interfere with or destroy, documents or electronic devices held in secure areas or,
- ⇒ Take documentation off campus without authorisation or,
- ⇒ Open Filing Cabinets, desk drawers, storage boxes, or anything which may contain personal data or,
- ⇒ Take pictures of, read, or download, any hard or soft copy information.
- ⇒ allow unauthorised persons access to any secure areas.

SPECIAL CATEGORY DATA relates to:

- ⇒ Racial or ethnic origin
- ⇒ Political opinions
- ⇒ Religious or philosophical beliefs
- ⇒ Trade Union membership
- ⇒ Genetic or biometric data
- ⇒ Physical or mental health
- ⇒ Sexuality or sex life

The rules for Special Category Data are stricter.

NOTE: Data relating to criminal convictions and offences, whilst not listed as a “special category”, has its own rules in the legislation.

DATA BREACH REPORTING

Examples of a data breach.

Lost USB keys/disks/laptops - given to person other than owner.

Exam Scripts or person specific correspondence left in classrooms or other public areas.

Medical Certificate/Documents left in public areas

Report to dp@ait.ie or call 0906468009

ACCOUNTABILITY AND RESPONSIBILITY

PRINCIPLES OF GDPR—Data should be:

Processed lawfully, fairly and in a way that is transparent to the data subject (“**lawfulness, fairness and transparency**”);

Collected, created or processed only for one or more specified, explicit and lawful purpose (“**purpose limitation**”);

Adequate, relevant and limited to what is necessary for those purposes (“**data minimisation**”);

Kept accurate and, where necessary, up-to-date (“**accuracy**”);

Retained no longer than is necessary (“**storage limitation**”);

Kept safe and secure (“**integrity and confidentiality**”)

PERSONAL DATA

Personal data is just that—personal. Only share necessary information with relevant people.

Online data protection training will be provided for you. You will receive an email in relation to this. The training is mandatory—and very straightforward.

There's More



WHAT IS PERSONAL DATA

Personal data is any information relating to an identified or identifiable natural person (data subject) – i.e: can be identified directly or indirectly by name, ref. no.; location data; online identifier, or by a combination of one or more factors specific to that person.

Examples are: Name, DoB, Address, Phone Number, IP Address (computer/phone) e-mail address; PPSn, etc...

Data relating to Health—including suspected cases of Covid 19—is confidential and described as special category personal data. Details made known to you should not be discussed outside of the relevant Institute staff. Your manager will advise you who the relevant Institute staff are.

DEFINITIONS

The GDPR (General Data Protection Regulations) applies to 'controllers' and 'processors'.

The Irish Data Protection Act 2018 is the Act which implements the GDPR in Ireland.

A controller determines the purposes and means of processing personal data. TUS is a data controller (this means all staff)

A processor is responsible for processing personal data on behalf of a controller – e.g confidential shredding

Data Subject – individual whose personal data is being processed

Recipient – person/authority to whom the personal data are disclosed

Third Party – a person/authority with whom data is shared who are approved to process personal data.

Consent—Unambiguous clear action which indicates that an individual gives

BREACH FINES—NOT FINE!

Up to €20,000,000 or 4% of Global turnover

Up to €10,000,000 or 2% of Global turnover

Public bodies – fine of up to €1,000,000

WHAT IS A DATA BREACH?

Personal data breach “means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” Find a list of data breach examples on www.ait.ie/gdpr!

RIGHTS SO!

- ◆ Data subjects have rights to:
- ◆ Ask,
- ◆ Be informed,
- ◆ Object to processing,
- ◆ Be forgotten,
- ◆ Correct Information and Restrict further Processing.

Check out www.ait.ie/gdpr for more information on data protection. Contact dp@ait.ie or phone 090 6468009.