## DATA BREACH INFORMATION SHEET

Current data protection law (GDPR, DPA 2018) require mandatory breach notification - breaches must be reported to the Office of the Data Protection Commissioner (DPC) within 72 hours, unless the personal data affected was anonymised or encrypted. As ‘*risk to the rights of the individual’* is broadly explained by *‘loss of control over personal data’* this will mean that most data breaches must be reported to the DPC.

Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned.

Failure to report a breach when required to do so could result in a fine for TUS, in addition to a fine for the breach itself.

**All breaches or suspected breaches should therefore be reported to TUS’s Information and Data Compliance Office without delay for assessment.**

**What is a "data breach"?**

The GDPR defines a data breach as “*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*".

## **EXAMPLES OF A DATA BREACH**

The following are examples of internal data breaches which should be reported to datacompliance@tus.ie. The majority of internal breaches reported are minor and are only recorded internally. Minor breaches are recorded anonymously where possible.

Reporting breaches internally has a number of important purposes.

1. It helps to identify issues at an early stage
2. It helps to improve the data protection processes within TUS

## Some examples of personal data (such as medical, financial, private information or private contact details) breaches include:

* Lost USB keys/disks/laptops - unencrypted.
	+ USB keys which are found should be handed in to the Information and Compliance office
* The sending of personal data to the unauthorised individuals.
	+ This includes personal data on unsecured email attachments or personal data in the body of an email.
	+ Sending (by post) personal data to the wrong address,
	+ Sending personal data via internal post to the wrong recipient.
* Loss of personal data to include:
	+ Emails containing personal data not received by addressee
	+ Post containing personal data not received by addressee
	+ Hard copy files containing personal data misplaced
* Sharing information outside of the purpose of collection of the data. The purpose of collection is generally documented in the Staff and Student privacy policies.
	+ Sharing with an unauthorised person/department within TUS
		- e.g. Pay claim sheet forwarded to Canteen instead of payroll
	+ Sharing with an unauthorised person/organisation outside TUS
		- e.g. Student details shared with an external marketing company
* Unlawful disclosure or destruction of personal data
	+ Sharing private contact details without consent
	+ Sharing personal data with unauthorised persons
	+ Giving student data to parents without consent
	+ Unauthorised access to soft/hard copy files, systems, or restricted areas of systems
	+ Deleting personal data which is required for processing of data subject contract.
* Inaccurate personal data leading to a breach (where correction to the data has been notified through the correct channels)
* Breaches of Physical security – e.g. Forced locks, doors, windows, filing cabinets.

Data shared appropriately to protect the vital interest of the data subject (i.e. life or death) is not a breach of personal data.

**If a data breach/suspected data breach is identified, please take the following steps**

**WITHOUT DELAY**

* Inform the Information and Data Compliance Office (datacompliance@tus.ie) and your Line Manager/Head of Functional Area.
* Email the datacompliance@tus.ie immediately and provide the following details:
	+ Your contact details (for follow up on the breach)
	+ Date and Time of data breach
	+ Is the breach ongoing
	+ Details of the breach

**How can I avoid a data breach?**
Data breaches can be caused by many factors, however some are more likely to occur than others. High standards of security are essential when dealing with all personal information. The following are guidelines in work practices which help to considerably reduce the risk of a data breach:

## **What you can do:**

* Keep personal data only on electronic devices that are:
	+ Password protected and never use your TUS password for any other account
	+ Regularly scanned with security software
	+ Portable electronic devices must be encrypted
* Leave paper documents containing personal data:
	+ If not in use, locked away
	+ Never lying around or behind
	+ Out of sight of unauthorised people (e.g. when reading a CV in a public place, on a train or in an airplane)
* After the original purpose you got permission for has come to an end, dispose of personal data, both electronic and paper, only in a manner that does not allow undoing deletion/destruction. This means for paper documents confidential shredding, and for electronic data using an appropriate deletion programme. The ‘Recycling Bin’ of your electronic device is not an appropriate place for deleted personal information.
* Check names on emails **before** sending – if in doubt ask!
* Keep circulation lists up to date
* Check consent status on ‘consent based’ lists

## **What to avoid**

* Never store personal information on any device that can be lost or stolen easily. This includes USBs, external hard disks you transport regularly, laptops in unsecured places, mobile phones, tablets.
* Storage solutions like Drop Box, Google Drive, etc. must not be used for personal data and are not supported
* Don’t log on to public Wi-Fi, e.g. (at airports, cafes, trains, etc.). This is more susceptible to hacking.
* Don’t use your TUS password for anything else
* For paper documents containing personal information:
	+ Never keep them on an open shelf in a general office
	+ Never throw them in the general bin
	+ Never leave them behind after you are finished with them
* Avoid sharing personal information – e.g. personal email address; mobile number; PPS Number, unless you have the specific right to do so.
* Don’t ask for personal information you don’t have the right to have.
	+ Ask yourself why you need the personal data.