DATA SHARING GUIDANCE February 2023

PURPOSE

The purpose of this document is to provide guidance to all University staff and faculty on best practice in relation to sharing personal and confidential data.

WHAT IS DATA SHARING

Data sharing is the process of providing data (confidential or personal data) to third parties. There are a variety of legitimate reasons to share data inside and outside of the University, ranging from regulatory requirements such as HESA, sharing vital information with authorities such as the Police and sharing student data with Partner Universities

GOLDEN RULES OF DATA SHARING

When sharing data, it is important to consider these Golden Rules:

Data privacy law is not a barrier to justified information sharing.

Be open and honest with individuals before sharing their information.

Seek advice from colleagues and the DPO if unsure.

Ensure the recipient is authorised to access the data.

Ensure the sharing is lawful, this could include:

- Gaining consent to share from the individual – if appropriate
- Requirement based on protecting the safety (vital interests) of an individual
- Requirement based on law, such as assisting court proceedings

Ensure the sharing is :

- **NECESSARY** – it is required as part of the process
- **PROPORTINATE** – sharing of the data is the right thing to do
- **RELEVANT** – the shared data is relevant and not excessive
- **ADEQUATE** – the recipients are authorised to access the data
- **SECURE –** the security of the sharing technology is appropriate for the data type

Maintain a record of the sharing and decisions behind it.

BEST PRACTICES FOR DATA SHARING

The ways in which we are able to share data internally and externally are vast, ranging from paper format through to encrypted digital systems. The below best practices should be considered when sharing data:

Consider the tool – As there are a variety of tools that can be used to share data, it is important to use the right tool for the job. The below table gives an idea of the commonly used tools across the University and their use cases. The general principle to align too is ensuring the most secure tool is used of the most sensitive data.

Encrypt, encrypt, encrypt – Most digital platforms come with a baseline encryption capability, if you are sharing sensitive data, check that the tool being used benefits from encryption, IT can help with any queries here.

Password protection – Where files contain sensitive data it is worth considering if password protection for the file itself is appropriate, most file types offer this capability built in.

Marking documents sensitivity – If a document is sensitive in nature, it should be marked as such, its also important to make sure the recipient is aware of this sensitivity, such as adding a sensitive marker to an email being sent.

Share links not documents – If a document is being shared internally, it is best to do this by sending a link to that document rather than a copy of it. It is a common practice to send copies of documents via email, the concern is that this document is now no longer under your control and collaboration becomes problematic.

BEST PRACTICES FOR WORKING WITH DATA

It is important to remember that when working with personal and confidential data we should be considerate and professional at all times. This is especially important where we are working with the personal data of colleagues, students or third parties.

We should consider that individuals have a right to access their own personal data if they chose to exercise it and, as such we need to ensure that this data is accurate, appropriate and work with it in a professional manner. This is especially important when working in email as this medium is not exempt from access to individuals that wish to have a copy of their data. This means email communications should retain a high level of professionalism and the content should remain objective and fact based wherever possible.

This same consideration also extends to any messages sent and received within chat platforms such as Microsoft Teams.

UNIVERSITY TOOLS USAGE

The below table provides guidance on the use cases for the commonly used tools across the University:

Tool	Type	Scenario	Use
E-mail	Communication	Internal to the University	Messages and data files containing personal and sensitive (special category) data - **Not a document store**
		External with public	Messages and data files containing personal data - **Not a document store**
SharePoint	File Sharing	Internal to the University	Document store for personal and sensitive (special category) data – **Permissions appropriate to role**
Blackboard	Learning Platform	Internal to the University	To collaborate and communicate with Students on learning matters
Teams	Messaging/Communication	Internal to the University	Messages, conferencing and data files, may contain personal or sensitive (special category) data
		External with public	Messages and conferencing, may contain personal data – **Not a file transfer mechanism outside of the University**