Research Data Collection and Storage when Working Remotely

Working remotely may create new challenges for researchers collecting, processing and storing data. Data collection can occur in many different ways, varying by discipline, methodology and research project. While working remotely it is important to ensure that we maintain the University's high standards of data management to ensure that all data is handled in a reliable, secure and compliant manner.

The checklist below provides guidance on selecting and using appropriate technologies to support your research activities while working remotely.

First Understand your Compliance Responsibilities

Everyone undertaking research involving personal data should make sure they are in compliance with the General Data Protection Regulation (GDPR) and, if applicable, the Health Research Regulations.

The University Data Protection Office provides information on the legislation and guidance on whether a Data Protection Impact Assessment is required to identify any data privacy risks which may arise from the activity.

Next Stay Secure

When working with research data you should ensure that you are protecting the data correctly. IT Services provides comprehensive information on how to ensure that your personal computing environment, your computers, mobile devices, removable storage devices are all configured securely and protected from loss or theft by appropriate technologies.

If working with personal data you may find it useful to identify and classify all the personal data that you are working with, documenting the appropriate technical and organisational security measures that you are putting in place to protect the data.

Use Research Technologies Supported by IT Services

The easiest way to ensure that you are using safe, secure and GDPR compliant tools is to use technologies provided and supported by IT Services.

The table below lists the main technologies available with a description of how you might use them to enable your research data collection and storage activities.

Technology	Description	Available to
Microsoft Forms	Data Collection: Microsoft Forms is a simple, lightweight app that lets you easily create surveys, quizzes, and polls, you can invite others to respond to it using any	• Staff • Students

	web browser, even on mobile devices. As results are submitted, you can use built-in analytics to evaluate responses. Form data, such as quiz results, can be easily exported to Excel for additional analysis or grading.	
Microsoft Teams	Data Storage: Microsoft Teams provides staff & students with a central place to work together online, with files kept in cloud storage, chat, project planner, wiki and other productivity tools.	• Staff • Students
Video conferencing in Microsoft Teams	Data Collection: Teams can be used to facilitate remote video conferencing meetings with colleagues or collaborators or Research interview participants who are working in different physical locations. A laptop or mobile device which is equipped with a camera and microphone is required. Automated interview transcription functionality is also available. For instructions, view the Meetings and Calls with Microsoft Teams - Getting Started Guide.	• Staff
Microsoft OneDrive	Data Storage: Microsoft OneDrive provides staff & students with 1TB of personal cloud storage. The service provides storage for many types of files, word documents, pdfs, folders, photographs, video files, etc. Access to data is available on campus or off campus without need of a VPN.	• Staff • Students
Microsoft SharePoint	Data Storage: SharePoint Online sites can be used to facilitate communications, data storage and collaboration for research projects or groups. Researchers can share reports and collaborate with Staff, students or create accounts for external collaborators.	• Staff • Students
Network Attached Storage	Data Storage: The NAS (Network Attached Storage) service allows staff and students in Trinity to store data on a central network server. The service can be accessed on and off campus (via VPN for staff), and is ideal for storing and sharing large data sets.	• Staff • Students
REDCap	Data Collection and Storage: REDCap is a web-based application for managing online surveys and databases. Managed instances of REDCap can be provided by the Research IT Group on request.	• Staff
Custom Web forms and Databases from Research IT	Data Collection and Storage: The Research IT group in IT services offer a number of Trinity wide and consortia/project specific storage facilities and data management services, customised solutions and general consultancy on best practice research data management is available.	• Staff
MyTrinityApps	Data Analysis: MyTrinityApps is a service that gives easy access to a selection of the most popular academic software applications such as SPSS for use on your own	• Staff • Students

	laptop while you are connected to the internet off campus.	

Be aware that using Free IT Tools and Services may involve risk

Many useful services are provided free of charge on the Internet, these include consumer communications tools like WhatsApp or social media tools like Facebook or data transfer tools like Dropbox.

However, many free IT tools are not secure or GDPR compliant and may pose risk to the privacy and security of your research data and research data subjects.

Issues which may arise when using free IT tools include:

- Poor Security - Necessary IT security controls may not be in place, passwords may be weak, data may not be encrypted.
- Data Ownership Issues - The end user agreement in place for the service may transfer ownership of the data to the service provider or allow for access to the data by other third parties.
- Data Loss - Sporadic use of online tools by transient team members may lead to data becoming abandoned or forgotten in online storage or becoming inaccessible if credentials are lost.

IT Services encourages researchers to use approved, vetted services from the University, or where additional tools are required to purchase enterprise licences in accordance with the Trinity Cloud Computing Policy and Guidelines.

Assess the IT Security and GDPR compliance of other Technologies which you procure

When planning to purchase a software tool or service where data will be collected stored or processed researchers should ensure to perform appropriate due diligence. This is to ensure that the tool is suitable and that all University-controlled data will be adequately protected.

This can be done by reviewing the IT security and privacy measures or certifications which the provider has in place. IT service providers or software providers can demonstrate compliance with security and privacy in several ways.

It is recommended that researchers procuring new technologies should engage with the Data Protection Office - dataprotection@tcd.ie - as a first step for support and guidance. This support will include the following steps being taken:

- Review of the vendor agreement to ensure appropriate protections for University-controlled data;
- Review of the vendor Privacy Statement for compliance with GDPR;
- Consultation as to whether a Data Protection Impact Assessment is required (e.g. for high-risk processing);

- Review of the retention period in place for the data; and
- Review of the required IT Security controls and certifications in place in the software product or service, such as strong authentication, encryption, firewalls etc.

Review Relevant University Policies

There are a number of University policies which are relevant including:

- Policy on Good Research Practice
- Data Protection Policy
- IT Policies

Consider some Training

Relevant online training is available at:

- GDPR Online Training
- IT Security Awareness Training