Guidance for Protecting Maynooth University's Data When Working Remotely

Devices

- Maynooth University's Information & Data Security Policy and associated policies apply while working remotely. (https://www.maynoothuniversity.ie/information-security/policies)
- Ensure your device is used in a safe location, for example where you can keep sight of it and minimise who else can view the screen, particularly if working with sensitive or personal data.
- Apply the latest security patches and enable automatic updates on all university owned devices, consult with IT Services if you need assistance. (https://www.maynoothuniversity.ie/it-services/servicedesk).
- Do not download personal data to any mobile device or home computer unless the device is secure.
- Delete all personal data from the mobile device or home computer as soon as practical.
- Use effective security controls (such as multi-factor authentication and strong passwords) and, where available, encryption to restrict access to the device.
- Lock your device if you do have to leave it unattended for any reason.
- Do not have work sensitive conversations near voice-enabled smart assistant devices or sent, shared, accessed or edited using non-university approved applications.
- Online training in GDPR and Data Protection requirements is available at: https://www.maynoothuniversity.ie/data-protection/online-gdpr-training-staff.
- If a device is lost or stolen or there is a data security incident, you should immediately contact the Data Protection Officer or Information Security Manager by email: dataprotection@mu.ie.

Emails

- You must use your work email account (@mu.ie) rather than personal ones for university related emails.
- Before sending an email, ensure you're sending it to the correct recipient, particularly for emails involving personal data.
- Emails between staff should only be sent via MU email accounts.
- If you need to share personal data, you should do so by using university provided OneDrive solution.
- Beware of phishing emails especially related to the topic COVID-19, do not click on any links or open attachments from an unknown sender.

Cloud and Network Access

- Core services such as Email, OneDrive and Teams provided by the university must be used for university business. Personal email (e.g. Gmail, Hotmail etc.) and non-university approved cloud services (e.g. Google Apps, Dropbox, etc.) must not be used for university business.
- Back up your data to university approved OneDrive solution, consult with IT Services if you need assistance. (https://www.maynoothuniversity.ie/it-services/servicedesk)

Paper Records

- It's important to remember that data protection and data security applies to not only electronically stored or processed data, but also university data in a manual form (such as paper records).
- Where you are working remotely with paper records, take steps to ensure the security and confidentiality of these records, a) keep locked in a filing cabinet or drawer when not in use, b) dispose securely (e.g. shredding). If you do not have access to a shredder, paper records should be retained securely until such time as you can return to campus where they can be shredded, and c) ensure they are not left where they could be misplaced or stolen.

- If you're dealing with records that contain special categories of personal data (e.g. health data) you should take extra care to ensure their security and confidentiality, and only remove such records from a secure location when it is strictly necessary carry out your work.
- Where possible, you should keep a written record of which records and files have been taken home, in order to maintain good data access and governance practices.

If you have any queries, please email dataprotection@mu.ie

1st July 2020