UNIVERSITY of LIMERICK
OLLSCOIL LUIMNIGH

Reduce the risk a data breach

Be vigilant – Data breaches can be caused by many factors but the following TECHNICAL AND ORGANISATIONAL MEASURES and practical guidance can help reduce the risk of a data breach:

Training and Policy Awareness

- Complete UL online Data Protection training (Directions on how to access training available at www.ul.ie/dataprotection)
- Complete UL online Cybersecurity training
- be aware and adhere to UL Data Protection Policy, FAQ guidance etc – www.ul.ie/dataprotection
- Be aware and adhere to ITD regulations

Email Security

- Use BLIND CC in group emails
- Be wary of clicking "reply all" instead of "reply"
- Be wary of the "autopopulate" tool when entering a recipient name – ensure the correct email address is in the TO box.
- If you need to send personal data in an attachment ensure:
    - correct attachment is added to the email
    - attachment is password protected (provide password under separate cover e.g. by phone call)
- If you need to send large or sensitive datasets, use the HEAnet File Sender Service (choose encrypted option).

IT Security

- Do not put personal data a device that can be easily lost or stolen (eg USBs/ external hard drives you can carry around).
- Never leave laptops, tablets, mobiles etc. unattended in your car etc.
- Use ITD supported solutions only
- Do not use Google Drive, Drop Box etc. for personal data storage
- Do not log on to public WI-FI for processing personal data, e.g at airports, cafes, etc - it can be hacked easily
- When upgrading work PC / disposing of obsolete equipment ensure full data wipe is completed
- Use a timed screensaver on PCs, laptops;
- Use timed log-out eg on PCs, laptops, tablets, phones etc
- Reboot your work PC regularly to allow for security patches/updates.

Electronic devices which hold personal data: Ensure they are:

- Password protected
- Encrypted – do not transport personal data on unencrypted portable devices e.g. UBBs, laptops.
- Regularly scanned with up to date antivirus software
- Regularly backed-up
- Change your password on a regular basis.
- Never use your UL password for any other account.

last updated 1 March 2019

Paper documents which contain personal data:

- Lock away when not in use ('clean desk policy'),
- Keep out of sight of unauthorised personnel when both inside/outside the office (e.g. reading a CV on a train)
- Always destroy personal data by confidential shredding
- Do not put records with personal data in the general waste/recycling bin.

Organisational Security measures

- Restrict access to personal data on "**need to know**" basis; **Authorised staff** only
- Control access to the office e.g. keep doors locked etc.
- Public counters/ground floor offices – ensure no personal data is visible to the public (paper records / PC screen);
- If you carry documents containing personal data to a meeting outside the office ensure you bring all documents back.
- Clean desk policy: Keep printers, fax machines, filing cabinets pigeon holes and shredding bin away from public areas.
- If you are changing roles within the University e.g. moving to a different department – leave data/records relating to behind & delete/empty your email account of all data related to your previous role.
- Retain personal data for no longer than necessary; do not keep "just in case".
- Retain/dispose in accordance with Records Management & Retention Policy.