



Incident Reporting:

(Examples of reportable breach and security incidents)

- Accidental loss or deletion of information
- Accidental disclosure of information to unauthorised persons
- Inappropriate use of data (e.g. for personal or business reasons, or use in projects for which it is not authorised/approved for use)
- Loss or theft of a computing device, removable media or printed data
- Physical security breaches (e.g. intruders, unaccompanied visitors)
- Inappropriate disposal of information (e.g. confidential papers in a bin)
- Complaints from data subjects, members of the public, external contractors, consultants, suppliers, agencies or collaborators relating to information/data issues
- Complaints about external contractors, consultants, suppliers, agencies or collaborators relating to information/data issues
- Computer viruses, malware, hacking, or other electronic attack
- Data held/retained when no permission or legal basis exists to hold/retain it.
- The ongoing lack of appropriate resources to reduce risk, such as suitable equipment or security measures
- Any other material or potential breach of Department or University policy, or any legal, contractual or regulatory breach