Report a Personal Data Breach

What is a personal data breach?

A personal data breach is an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Breaches may be the result of accidental or deliberate causes. **A breach of personal data must be reported immediately**.

What must be reported?

Any information security incidents that has affected the confidentiality, integrity or availability of personal data, e.g.

- Personal data that has been lost, destroyed, corrupted or inappropriately disclosed.
- Personal data that has been accessed or shared without appropriate authorisation.
- Personal data that has become unavailable, where that unavailability has a significant negative effect on the subjects of the data.

Examples include, but are not limited to:

- Stolen or lost laptop, ipad or other mobile device holding personal data belonging to staff, students or work-related third parties such as contractors; including personal data in emails
- Sensitive personal data being made publicly available on a website
- Personal data emailed to inappropriate or incorrect recipients
- Alteration of personal data without appropriate authorisation.
- Malware has corrupted personal data
- Stolen or lost bag holding printed material that contains personal data
- Personal data transferred outside of EEA without authorisation or without using authorised transfer facilities

How do I report the data breach?

You should report personal data breaches to the University Secretary's office [dpo@uca.ac.uk] or by telephone x2603, using the form below. Only basic details are required to report the personal data breach.

- Respond to the questions from the online form. If submitting via email, provide an outline of what has happened or has been observed.
- Do not include any personal data involved in the incident.
- Support any investigation arising as fully as possible.

When do I report incidents?

- Incidents must be reported as soon as they are discovered.

Who should report?

- All employees, temporary workers and contractors including overseas agents
- All students, when engaged on a programme of study or when working for the University in a paid or unpaid capacity.
- Third parties, like data processors, should follow contractual obligations with regards to reporting breaches, which may be initially to their University contacts. It is the University contact that should then report within the University. Third parties should not report incidents directly as below unless contractually bound.

Why should incidents be reported?

- The longer an incident goes unreported, the longer a weakness may remain unaddressed allowing the incident to escalate or for further incidents to occur.
- The EU General Data Protection Regulations (GDPR) places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach. Fines will be imposed for late or non-reporting.
- Knowing that a breach has occurred and delaying reporting reduces the time available for the investigation team to understand and assist with a response and still meet legal compliance.
- Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust and so prevent future breaches.

What happens after the report is made?

- The University Secretary or her nominee will make an initial assessment to determine the next steps.
- The severity of the incident will inform and direct the appropriate level of leadership involvement.
- An investigation may be conducted using a variety of techniques and tools, including interviews, campus visits and forensic analysis.
- The outputs of the investigation may include corrective and preventive actions, formal reporting or other communications.

Personal Data Breach Report Form

Date and time of reporting	
Date and time incident occurred	
Date and time incident was discovered	
Name and Job Title of Person Reporting	
Contact telephone number	
Brief details of the incident, ie loss, corruption, accidental disclosure; location, and how the breach happened.	
Details of any personal data at risk, if known.	

Any actions taken to reduce the risks – either taken by the reporter or by others		
For use by the University Secretary's Office Only		
Report received by:		
Date and time of receipt:		
Action taken and by whom		Date of Action taken