Data Breach Notification Procedure

What is a data breach?

A "personal data breach" is defined in the General Data Protection Regulations 2016/679 (GDPR) as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly described as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Reporting a data breach

In the event that:

- you become aware of a data breach;
- you have a concern regarding a lapse in security that may result in a data breach,

you must notify the Data Protection Officer (DPO) (Ruth Cartwright on extension 2348 or at dataprotection@ucb.ac.uk) as soon as possible.

The information that you give should contain:

- the nature of the data breach (e.g. I lost my USB in a lecture theatre and it contains personal data);
- the type of personal data that is held (e.g. names, addresses, emails, grades);
- how sensitive you feel the information is (e.g. could the contents be used to cause harm/distress to the individual, or to contact them without their consent);
- whether the data was encrypted; and
- how many individuals will be affected by it.

You will be asked to complete a Data Breach Form which can be found at: https://www.ucb.ac.uk/about-us/data-protection-resources.aspx under staff resources. Once this information has been obtained, the Data Protection Officer will investigate and gather as much information as possible and assess whether the ICO must be notified.

This will be done by ascertaining the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk to the individual(s) affected then UCB must notify the ICO.

In assessing risk to rights and freedoms, UCB will focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

If the risk of damage to individuals is unlikely then it will not be reported, but will be dealt with internally. The justification for not notifying the ICO of a data breach will be documented.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, UCB will also inform those individuals affected by the breach without undue delay.

UCB is obliged to make the appropriate notifications within a very limited time period and the penalties to UCB for non-compliance can be severe. Therefore, it is very important that you inform the DPO as soon as you suspect or know that a personal data breach has occurred.

You must retain all evidence relating to personal data breaches, in particular, to enable UCB to comply with its obligations under the GDPR to maintain a record of the facts of any personal data breach, its effects and the remedial action taken.

Once the ICO (if applicable) has been informed, full investigations will be undertaken to ascertain how the breach took place and we can strengthen our technical and organisational measures to prevent further data breaches of this nature in the future.

Date Last revised: 30/04/2020