Data Breach Guidance

What is a personal data breach?

A data breach occurs when personal data that the University is responsible for is subject to unauthorised destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to.

Personal data is data that relates to a living individual and includes information that affects the person's privacy in personal or family life, or in a business or personal capacity.

What should I do when a data breach takes place or I think one might have happened?

If you think there may have been a data breach, you should report it to the Information Governance Officer. They will then be able to assess the significance of the breach. The data protection officer should:

- Take steps to attempt to contain and recover the personal information where possible
- Report to the Information Governance and Complaints Officer(Data Protection Officer) at dp@rgu.ac.uk on the nature of the breach, the risks of re-occurrence and impact upon University operations.
- The Director of Planning & Policy Development, in consultation with the DPO, assess whether it is necessary to notify the Information Commissioner's Office (ICO) or the individuals affected, about the breach and also whether to convene a breach investigation panel.

Such a panel may consist of, amongst others:

- The Director of Planning & Policy Development
- University Solicitor
- Data Protection Officer
- Head of Human Resources

The panel will consider;

- Whether a breach has occurred
- How that breach arose
- What action, if any should be taken to avoid future occurrences
- Whether any action should be recommended against any member of staff or student
- The effectiveness of the University's response to the breach.

Suspected serious data security breaches require the University to investigate and contain the situation and also draw up a recovery plan which will include where necessary any damage limitation.

Risk assessment of data breach

Before deciding what further steps are necessary, the data protection officer in conjunction with relevant other staff will assess the risks which may be associated with that breach. The following factors should be considered:

- What type of data is involved?
- How sensitive is it?
- If data has been lost or stolen, are there any protections in place such as encryption
- What has happened to the data?
- What could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence?

Other considerations include:

- Are there any legal or contractual requirements?
- Can notification help the University meet its security obligations?
- Can notification help the individual manage the risks for example by cancelling a credit card or changing a password?
- How can notification be made appropriate for particular groups of individuals, for example, children or vulnerable adults?
- Who will the University notify, what will they be told and how will the message be communicated?
- Who else should be notified, for example third parties such as the police, insurers, professional bodies, bank or credit card companies?

When do individuals have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What if the breach is not 'high risk' to an individual?

Under the GDPR, the University has a duty to report certain types of data breaches to the Information Commissioner's Office (ICO). A breach must be reported when it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals, for example discrimination, loss of confidentiality or any other significant economic or social disadvantage. When a data breach occurs, the information governance officer will co-ordinate if a notification to the ICO should occur.

What information must a breach notification contain?
A notification to the ICO must contain:

- The nature of the personal data breach including;
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the data protection officer (Information Governance Officer) or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify a breach?
A notifiable breach has to be reported to the relevant supervisory authority (ICO) within 72 hours of the University becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time period and allows you to provide information in phases.

Early notification to the university's Data Protection Officer is imperative to ensure a required notification to the ICO can be made.

All notifications will be done by the university's Data Protection Officer (Information Governance and Complaints Officer)

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without delay.

Failing to notify a breach when required to do so can result in a significant fine.