Reporting a Personal Data Breach Procedures

Procedure name:	**Reporting a Personal Data Breach**
Procedure reference:	**Pro-DB-GDPR**
Created by:	**Data Protection Officer**
Approved by:	**Executive Leadership Team**
Date of last review:	**July 2021**
Date of next review:	**July 2022**
Revision number:	**5**

This document is available in other formats including audio, Braille and other languages. The same applies to all material which is referenced within in it. For further assistance, please contact the Quality Department on 01925 494645 or email quality@wvr.ac.uk

Contents

1. Purpose

The purpose of this procedure is to set out the steps that need to be taken in the event of a personal data breach to ensure timely reporting. The procedure seeks to ensure that the College is compliant with the Information Commissioner's Office deadline for reporting personal data breaches within 72 hours.

2. Scope

This procedure applies to all staff, Governors, volunteers, student placements, subcontractors and students for designated courses at the College.

3. Responsibility

Ultimate responsibility for this procedure within the College lies with the Data Protection Officer.

4. Procedure

4.1 What is a personal data breach?

A personal data breach means 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. A breach is more than just about losing personal data.

Examples of 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.

4.2 Reporting a personal data breach

A personal data breach needs to be reported immediately to the College's Data Protection Officer. The Data Protection Officer needs to notify the Information Commissioner's Office of a breach within 72 hours of the time when the breach occurred, therefore, the Data Protection Officer needs to be notified as soon as possible.

4.3 Information required when reporting a personal data breach

When reporting a breach, you must provide:

- a description of the nature of the personal data breach including, where possible:
- when and how you found out about the breach;
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects;
- the details of any policies or procedures relevant to the incident;
- whether the data has now been recovered

4.4 Telling others about a personal data breach

The Data Protection Officer will advise you when reporting a personal data breach whether those impacted by the breach need to be notified.

If the individuals impacted by a personal data breach need to be informed, you need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer (Tracy Callaghan, tcallaghan@wvr.ac.uk) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

In the event of a personal data breach, you also need to consider whether you need to notify third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

4.5 What happens if we fail to notify the Information Commissioner's Office of a personal data breach

Failure to notify a breach to the Information Commissioner's Office when required to do so can result in a significant fine.