# Coventry University
## Data Breach Policy and Procedure

**Contents**

1. Introduction 2
2. Purpose & Scope 2
3. Data Breach 2
4. Examples of Data Breaches 2
5. Procedure for reporting a data incident breach 3
6. Breach Notification - Coventry University to Data Subject 3
7. Breach Notification – Coventry University to ICO 3
8. Enforcement 4
9. Policy Review 4
Introduction

This document sets out the policy and procedures for data breach incidents and must be read in conjunction with the University Group’s Data Protection Policy. See link below.

https://share.coventry.ac.uk/students/Registry/_layouts/15/WopiFrame.aspx?source doc=/students/Registry/Documents/Data_Protection_Policy.docx&actio n=default

Purpose and Scope

The purpose of this document is to provide a framework within which the University will ensure compliance with the requirements of a data breach incident.

This policy applies to University staff, agency workers, student ambassadors, contractors and third party agents who process data for or on behalf of the University and it must be complied with in the event of a data breach.

Data breach

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft of personal data, or unauthorised access to personal data.

Examples of Potential Causes of Data Breaches

- Loss or theft of data or equipment on which data is stored (e.g. loss of paper record, laptop, iPad or unencrypted USB stick) compromising personal data.
- Inappropriate access controls allowing unauthorised use (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems) compromising personal data.
- Equipment failure leading to a data breach and compromising personal data
- Human error leading to a data breach and compromising personal data
- Unauthorised disclosure of information compromising personal data (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee)
- Unforeseen circumstances such as a fire or flood leading to a data breach and compromising personal data
• Hacking attack leading to a data breach and compromising personal data

• ‘Blagging’ offences where information is obtained by deceiving the organisation which holds it

**Procedure for reporting a data breach incident**

The primary point of contact for reporting a data breach incident is the Group Data Protection Officer in the Information Protection Unit (IPU).

Data breach incidents should **upon discovery** be **reported immediately and without delay** to the Data Protection Officer in Information Protection Unit by emailing **ac1212@coventry.ac.uk** and **enquiry.ipu@coventry.ac.uk**.

The responsibility for reporting the breach lies with the member of staff who discovered the breach.

As part of the reporting procedure a data breach form must be completed.

When a data breach is reported the IPU will send out a Data Breach Form with a unique reference number for you to complete which needs to be completed and returned as a matter of urgency and in any event by close of business on the next working day.

The DPO will inform the Deputy Vice-Chancellor (Strategic Alignment and External Relations) of the breach as soon as reasonably practicable after it is reported.

The DPO will investigate the breach and where appropriate the DPO will notify line management and the People Team of the breach.

**Breach Notification - Coventry University to Data Subject**

Where the personal data breach is likely to result in impacting the rights and freedoms of the data subject the University shall notify the affected data subjects without undue delay, in accordance with the Data Protection Officer's recommendations.

**Breach Notification – Coventry University to ICO**

The DPO will notify the ICO without undue delay, of a personal data breach where legally required to do so.
Enforcement

Failure to adhere to this policy, the delay in reporting the breach to the DPO and non-reporting of breaches will be addressed by necessary disciplinary actions in accordance with the University's Staff Disciplinary Procedures.

Policy Review

This policy will be reviewed every year or where significant legal changes have occurred.

| Version Control | 1 |
| Responsibility of | Information Protection Unit |
| Approval date | 31 May 2017 |
| Reviewers | Group Data Protection Officer  
Head of Information Security  
Senior Solicitor |
| Date of commencement | 1 June 2017 |
| Approved by | Information Protection Committee |
| Review date | 31 May 2018 |
| Related Policies, Procedures, Guidance, Forms or Templates | Data Protection Policy |