Aston University
BIRMINGHAM UK

# Personal Data Breach Notification Procedure

## 1. Scope of the Procedure

### 1.1 Purpose of the Procedure

Compliance with this procedure is required to ensure the University's compliance with data protection law and particularly the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("the UK GDPR"), which require personal data breaches to be reported to the relevant supervisory authority. Failure to comply with this legislation can result in financial penalties being levied against the University.

This procedure should be read in conjunction with the Privacy Policy.

### 1.2 What is covered by the Procedure

This procedure applies when a personal data breach has been detected.

### 1.3 Who is covered by the Procedure

All those who access personal data held by the University including staff must familiarise themselves with this procedure and comply with it when dealing with personal data.

Failure to comply with the procedure with be dealt with in accordance with the Privacy Policy and may involve disciplinary action.

## 2. Detailed Procedures Statement

2.1 By law, a personal data breach must be reported to the Information Commissioner's Office where it is likely to result in a risk to the rights and freedoms of data subjects. Such a breach must be reported within 72 hours of discovery. All suspected personal data breaches must be reported to the Data Protection Officer at dp_officer@aston.ac.uk immediately.

2.2 A notification of a personal data breach to the Information Commissioner's Office must include the following:

- a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer;
- 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.

2.3 If, in the opinion of the Data Protection Officer, a breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will provide the draft breach notification and any supporting documents to Chief Operating Officer (or another member of the University Executive if the Chief Operating Officer is unavailable). The Chief Operating Officer will consider if

the breach is likely to result in a risk to the rights and freedoms of data subjects and therefore determine whether to submit the report to the Information Commissioner's Office.

2.4 If the breach is likely to result in a high risk to the rights and freedoms of data subjects, then the data subject/s concerned will be informed of this directly and without undue delay. The University will provide the following information to the data subject/s concerned:

- the name and contact details of the Data Protection Officer;
- 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 the measures taken to mitigate any possible adverse effects.

2.5 For all personal data breaches, the Data Protection Officer (or their nominee) will document the circumstances of the breach, its effects and any remedial action taken in the Register of Personal Data Breaches.

2.6 For all personal data breaches, the Data Protection Officer will consider whether it is necessary to notify any third parties such as the police, insurers, professional bodies, or bank or credit card companies of the breach in order to reduce the risk of financial loss to data subjects.

2.7 The Data Protection Officer (or their nominee), in consultation with relevant University colleagues, will investigate the cause of the breach and identify any remedial steps that might be necessary to prevent a recurrence.

3. **Version Control**

| Reference No. | Version | Executive Sponsor | Officer Responsible | Consultation Process | Effective Date |
|---|---|---|---|---|---|
| BNP001 | 1 | Chief Financial Officer | Head of Legal Services | GDPR Working Party | 24 May 2018 |
| BNP001 | 1.1 | Chief Operating Officer | General Counsel | Chief Operating Officer | 1 February 2019 |
| BNP001 | 1.2 | Chief Operating Officer | General Counsel | Information Security & Compliance Group | February 2021 |