University of Bolton

Teaching Intensive, Research Informed

DATA BREACH MANAGEMENT PROCEDURE

1. Introduction

1.1 The University collects, holds, processes and shares large amounts of personal data and has an obligation to ensure that it is kept secure and appropriately protected.

2. Purpose

2.1 The purpose of this procedure is to ensure that:

- personal data breaches are detected, reported, categorised and monitored consistently
- incidents are assessed and responded to appropriately without undue delay
- decisive action is taken to reduce the impact of a breach
- improvements are implemented and communicated to prevent recurrence or future incidents
- certain personal data breaches are reported to the Information Commissioner's Office (ICO) within 72 hours, where required

2.2 This document sets out the procedure to be followed to ensure a consistent and effective approach in managing personal data security breaches across the University.

3. Scope

3.1 This procedure applies to all staff, students, partner organisations and partner staff, suppliers, contractors, consultants, representatives and agents that work for or process, access, use or manage personal data on behalf of the University.

3.2 This procedure relates to all personal and special category ('sensitive') information handled, stored, processed or shared by the University whether organised and stored in physical or IT based record systems.

4. Definition

4.1 A personal data breach means ***'a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.***

4.2 A personal data breach in the context of this procedure is an event or action that has affected the confidentiality, integrity or availability of personal data, either accidentally or deliberately, that results in its security being compromised, and has caused or has the potential to cause damage to the University and/or the individuals to whom the information relates to.

4.3 For the purpose of this procedure a data security breach includes both confirmed and suspected breaches.

4.4 A data breach incident includes but is not limited to:

- Devices containing personal data being lost or stolen (e.g. laptop, USB stick, iPad/tablet device or paper record)
- Access by an unauthorised third party or unlawful disclosure of personal data to a third party

- Deliberate or accidental action (or inaction) by a data controller or processor
- Sending personal data to an incorrect recipient
- Alteration of personal data without permission
- Loss of availability of personal data
- Data input error / human error
- Non-secure disposal of hardware or paperwork containing personal data
- Inappropriate access/sharing allowing unauthorised use of, access to or modification of data or information systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

5. Reporting an incident

5.1 The University adopts a culture in which data protection breaches are reported. Any student, staff, contractor, partnership organisation, partner staff or individual that processes, accesses, uses or manages personal data on behalf of the University is responsible for reporting information security incidents and data breaches immediately or within 24 hours of being aware of a breach to the **Head of School/Centre/Department**, **Data Protection Officer** at dpo@bolton.ac.uk, **Head of Information Systems and Technology** and **Registrar** who will investigate the potential breach.

5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

5.3 A Data Breach Report Form (see Appendix 1) should be completed as part of the reporting process. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information and how many individuals are involved.

6. Containment and Recovery

6.1 The Data Protection Officer in liaison with the Head of Information Systems and Technology and Registrar will determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An initial assessment will be made to establish the severity of the breach, who will take the lead as designated Investigating Officer to investigate the breach (this will depend on the nature of the breach) and determine the suitable course of action to be taken to ensure a resolution to the incident.

6.3 The Investigating Officer will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.4 The Investigating Officer will establish who may need to be notified as part of the initial containment.

6.5 Advice from experts across the University such as IT, HR and legal and in some cases contact with external third parties may be sought in resolving the incident promptly.

7. Investigation and Assessing the Risks

7.1 An investigation will be undertaken by the Investigating Officer immediately and wherever possible within 24 hours of the breach being discovered/reported.

7.2 The Investigating Officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how likely they are to happen and how serious or substantial they are.

7.3 The level of risk associated with a breach can vary depending on the type of data and its sensitivity. The investigation will need to consider the following:

- What type of data is involved?
- How sensitive is the data?
- Where data has been lost or stolen are there any protections in place such as encryption?
- What has happened to the data? Has it been lost or stolen?
- Could the data be put to any illegal or inappropriate use?
- Could it be used for purposes which are harmful to the individuals to whom the data relates?
- How many individuals' personal data has been 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?

8. Notification of Breaches

8.1 The Investigating Officer in consultation with the Data Protection Officer, Head of Information Systems and Technology and Registrar, will determine who needs to be notified of the breach.

8.2 Any notification must be agreed by the Head of School/Centre/Department and Registrar.

8.3 Every incident will be assessed on a case by case basis. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

The following will need to be considered:

- Are there any legal/contractual notification requirements?
- Can notification help the individual? Could they take steps to act on the information to protect themselves?
- Would notification help prevent the unauthorised or unlawful use of personal data?
- Can notification help the University meet its obligations under the data protection principles?
- Is there a large number of people that are affected? Are there serious consequences?
- Should the ICO be notified[1] of the personal data breach? If so, notification shall be within 72 hours with details of:

  (a) a description of the nature of the personal data breach including, where possible:

    - the categories and approximate number of individuals concerned; and

[1] The ICO must be notified where there is likely to be a risk to people's rights and freedoms.

The risk to people's rights and freedoms could be physical, material or non-material damage to a person such as loss of control over their personal data or limitation of their rights. Discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to a natural person.

- the categories and approximate number of personal data records concerned;

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) details of the security measures and procedures in place at the time the breach occurred; and

(e) 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.

8.4 If the University decides not to report the breach to the ICO it will need to be able to justify the decision and document it. Failing to notify a breach when required to do so can result in a significant fine up to ***€10 million*** *or* ***2% of the University's turnover*****.**

8.5 If a breach is likely to result in a high risk to the rights and freedoms of individuals, notification to the individuals whose personal data has been affected by the incident must be **without undue delay** describing:

- the nature of the personal data breach;
- the name and contact details of the data protection officer 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 including what action the individual(s) can take to protect themselves.

The following factors to consider include:

- Sensitivity of information
- Volume of information
- Likelihood of unauthorised use
- Impact on individual(s)
- Feasibility of contacting individuals

8.6 If the University decides not to notify the individuals affected, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

8.7 The Investigating Officer and/or Data Protection Officer and Registrar must consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can help reduce the risk of financial loss to individuals. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.8 The Investigating Officer and/or Data Protection Officer will consider whether the [**marketing and communications team]** should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.9 All personal data breaches and actions will be recorded by the Data Protection Officer regardless of whether or not they need to be reported to the ICO.

9. Evaluation and Response

9.1 Data protection breach management is a process of continual review. Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 The review will consider:

- Where and how personal data is held/ stored.
- Where the biggest risks lie and identify any further potential weak points within its existing security measures.
- Whether methods of transmission are secure; sharing minimum amount of data necessary.
- Staff awareness

9.4 Regardless of the type and severity of incident, there will always be recommendations to be made even if it is only to reinforce existing procedures. There are **two** categories of recommendation that can be made:

Local: these apply purely to the School/Centre/Department affected by the incident and will usually reflect measures that need to be taken to restrict the chances of the same type of incident occurring.

Organisational: some incidents will be caused by factors that are not unique to one School/Centre/Department but can be found across the University. Issues such as training, information handling and physical security affect all Schools/Centres/Departments and it is essential that the University identifies such risks and puts in place measures to prevent the incident occurring elsewhere.

9.5 All recommendations will be assigned an owner and have a timescale by when they should be implemented which has a dual purpose. The first is to ensure that the University puts in place whatever measures have been identified and that there is an individual that can report back to the Data Protection Officer on progress. The second is that where incidents are reported to the ICO, the University can demonstrate that the measures have either been put in place or that there is a documented plan to do so.

9.6 Identifying recommendations is more than just damage control. The knowledge of what has happened together with the impact is a fundamental part of learning and continual improvement which can then be disseminated throughout the University.

APPENDIX 1

DATA BREACH REPORT FORM

Complete Section 1 of this form and email it to:

- **Data Protection Officer dpo@bolton.ac.uk**
- **Head of Information Systems and Technology P.OReilly@bolton.ac.uk**
- **Registrar s.duncan@bolton.ac.uk**

Section 1: Notification of Data Security Breach **To be completed by Head of School/Centre/Dept. of person reporting incident**	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name and contact details of person reporting incident (email, address, telephone number):	
Brief description of incident or details of the information lost:	
Number of people affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity **To be completed by the Investigating Officer with the Head of School/Centre/Dept. of the area affected by the breach and IT where applicable**	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Special category 'sensitive' personal data** (as defined in the relevant data protection law(s)) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) genetic or biometric data; f) commission or alleged commission of any offence, or g) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. • Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; • Personal information relating to vulnerable adults and children;	

• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; • Spreadsheets of marks or grades obtained by students, information about individual cases of student disciplinary or sensitive negotiations.	
• Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken **To be completed by Data Protection Officer and/or Investigating Officer**	
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Investigating Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Investigating Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on: Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**