**Data Breach Policy**

**Introduction**

Queen’s University Belfast is committed to safeguarding staff, students, external partners and individual service users, personal and sensitive data, in line with the Data Protection Act 2018 (“the Act”) and the General Data Protection Regulation (GDPR).

Part of this commitment is ensuring that we fulfil our duties and obligations as a Data Controller to living persons and the national supervisory authority, the Information Commissioners Office (ICO). This includes the investigation, reporting and notification of any data breach in the official manner, as prescribed by the ICO, where there has been sufficient violation of the rights and freedoms of the data subject(s).

**Purpose and Scope**

The University has a legal obligation to notify the ICO of security incidents where the confidentiality, integrity or availability of personal data and/or sensitive personal data is affected, and where there is a high risk to the rights and freedoms of the data subject.

A personal data breach could be the result of a security breach 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 serious data breach may contravene both the Act and the internal Data Protection Policy. As a result, it could be considered as a disciplinary matter. It could also be considered a criminal matter for which the University, and the individual concerned, could be held criminally liable.

**Policy Statement and Objectives**

The objectives of this policy and associated guidance are to ensure that any and all data breaches are reported, investigated, documented and appropriate levels of notification are provided to the data subject and ICO where necessary.

To ensure that the policy objectives are met, the University will provide arrangements and procedures for the following;

* To capture the details of the breach when it is discovered
* The investigation into the breach
* The process for notification of relevant parties
* Further actions to limit or eliminate future breaches.

**Consultation**

The University has consulted with the ICO and Pinsent Masons for advice and best practice for breach notification processes.

**Equality and Diversity**

During consultation with Pinsent Masons, Section 75 of the Northern Ireland Act 1998 was addressed. This policy is institutional wide and encompasses all staff members, regardless of their age, religion, health, sexuality or ethnicity. Each individual is required, by law, to adhere to the Act and are contractually and duty bound to adhere to Queen’s policy and procedures in relation to Data breaches and wider data protection issues.

**Definitions and Types of Breach**

For the purposes of this policy, data breaches include both suspected and confirmed incidents.

An incident, in the context of this policy, is an event or action which results in the potential or actual destruction, loss, alteration, unauthorised disclosure of, or access to, personal and/or sensitive data, whether unlawful or accidental, and it has the potential to damage or cause harm to any natural persons, the University’s information assets, and/or reputation.

An incident includes but is not limited to, the following;

* Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB memory stick or paper record)
* Equipment theft or failure
* System failure
* Unauthorised use of, access to or modification of data or information systems
* Attempts (failed or unsuccessful) to gain unauthorised access to information or IT system(s)
* Unauthorised disclosure of sensitive/confidential data
* Website or online resource defacement
* Hacking attack
* Unforeseen circumstance such as fire or flood
* Human error
* Data quality – incorrectly entered or retrieved data items
* ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

**Reporting and Notification of Incident**

Any individual who accesses, uses or manages the University’s information is responsible for reporting a data breach and information security incidents immediately to your line manager or closest line of authority. For example, if a data breach is caused by a senior manager, they may contact the Data Protection Officer (DPO – Sandra McDonald – s.mcdonald@qub.ac.uk) and/or the data breach inbox (databreach@qub.ac.uk).

If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. This does not mean the next working day but as soon as the breach notification details can be sent to the required mailbox.

The notification should include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data is related to people, the nature of the information, and how many individuals are affected. A ‘Breach Notification Form’ should be completed as part of the reporting and notification process (refer to Appendix 1).

All staff should be aware that any data breach of personal or sensitive data may result in the University’s Disciplinary Procedures being instigated.

**Containment and Recovery**

The DPO and/or Data Security Manager (Chris Linton – c.linton@qub.ac.uk) will firstly determine whether the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effects of the breach.

An initial assessment will be taken by the DPO/Data Security Manager in liaison with the relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (LIO). This will depend on the nature of the breach and in some cases could be the DPO.

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

The DPO will establish who may need to be notified as part of the initial containment and will inform the ICO or Police, where appropriate.

Advice from persons across the University, including persons affected, involved or data security and systems experts, to help resolve the incident promptly.

The DPO and when appropriate the Data Security Manager will liaise with the LIO and any relevant persons involved in the breach or breach investigation, to determine the suitable course of action to be taken to ensure a resolution to the incident.

**Investigation**

An investigation will be undertaken by the identified LIO or in circumstances where by a senior manager is involved in the breach the DPO or members of the Information Compliance Unit, **within 24 hours of the breach being discovered or reported**.

The investigation will need to take into account the following:

* The type of data involved;
* Its sensitivity;
* The protections that are in place (e.g. encryption);
* What has happened to the data (e.g. has it been lost, modified or stolen);
* Whether the data could be used in illegal or inappropriate ways;
* Data subject(s) affected by the breach, number of individuals involved (or records involved) and the potential effects on the data subject(s);
* Whether there are wider consequences to the breach.

**Notification**

The Information Compliance Unit (ICU)/DPO must be notified as soon as the data breach is discovered. This will initiate the formal investigation process.

The DPO, in consultation with relevant colleagues and pending the investigation by the designated LIO, will establish whether the ICO will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Each incident will be reviewed on a case by case basis and will use the following to guide decisions on notification:

* Whether the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms under Data Protection legislation;
* Whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate the risks – change passwords etc.)
* Whether notification would help prevent unauthorised or unlawful use of data;
* Whether there are any legal or contractual notification requirements;
* No every incident requires or warrants notification and over notification may cause disproportionate enquires and work, whilst potentially causing needless concern or worry about personal data from the data subject themselves.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk adversely affecting that individual’s rights and freedoms, will be informed without undue delay. Notification will include a description of ho and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the University for further information or to ask questions on what has occurred.

The DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. 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.

The DPO and Registrar will consider whether the Communications Office should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A formal schedule of data breaches will be maintained by the Information Compliance Unit, whether notification is provided to the ICO or data subject or not.

**Evaluation and Response**

Once the initial incident is contained, the DPO 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.

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.

The DPO will consider;

* Where and how personal data is held and where and how it is stored
* Where the biggest risks lie including identifying potential weak points within existing security measures;
* Whether methods of transmission are secure; sharing minimum amount of data necessary;
* Staff awareness;
* Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by University Operating Board (UOB).

**Policy Review**

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

This policy was last reviewed in January 2020. The policy was approved by the UOB and Registrar in January 2020.

|  |
| --- |
| **Breach Notification Queen’s University Belfast** |
| Nature of breach:    |
| Categories of Data Subjects (student, staff, etc.):  | Approximate number of Data Subjects:  |
| Categories of Personal Data Records (health, financial, etc.): | Approximate number of Personal Data records:  |
| Investigating Officer(s)/Point of contact (can be more than one):  |
| Potential consequences of breach:  |
| Initial containment or retrieval actions: |

**Appendix 1** Breach Notification Form

|  |  |
| --- | --- |
| **Reference #:**  | **Service Affected:**  |
| **Criticality (H/M/L):** |  |
| Description of Incident – including impact (who was affected, what systems were affected, scale of impact) |
| Timeline of Events – include all relevant events and meetings to resolve issues. |
| Investigation of Incident – include findings and results of the investigation |
| Resolution and Conclusions |
| Recommendations/Lessons learned |
| In the event of any reoccurrence, what action can staff take to reduce the impact? |
| Report completed by:  |
| Date:  |

**Appendix 2** Incident Report Form

**APPENDIX 3**

