St Mary's University College Belfast
A College of Queen's University

# Data Breach Management Procedure

---

**BACKGROUND**

As a Data Controller the Higher Education Sector must obtain, manage, process and store all data in compliance with the UK General Data Protection Regulations (GDPR) and its 7 main principles.

***Article 5 (1) of the GDPR states personal data must be**:*

*"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');*

*(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');*

*(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

*(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

*(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');*

*(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

*Article 5(2) adds that:*

*"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."*

## Failure to report a breach

The General Data Protection Regulation requires a greater degree of accountability for organisations handling personal data. As part of the ICO regulations, a personal data breach must be reported to the Information Commissioners Office within 72 hours.

Failure to comply with the principles may leave the College open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.

'*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.'*

The College will provide Data Protection training and approved policy and procedures to assist staff in minimising the risk of theft, unauthorised access, loss and damage while fulfilling their contracted duties.

### 1. SCOPE

This procedure applies to all staff, students, contractors, and third-party vendors who have access to university systems and data. It covers breaches related to all data types including personal, financial, academic, and administrative information.

Should a member of staff suspect a breach has occurred, they are responsible for notifying his/her line manager and the College Data Protection Officer (DPO).

Once the suspected breach has been reported to the College DPO, the procedure's scope is limited to the DPO or delegates.

### 2. PROCEDURE

The College must establish a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. **Immediately, and without delay,** contact the Data Protection Officer. In the event of a sufficiently serious data breach, the College will notify those affected without undue

delay. Please find details of real-life examples of data breaches that have occurred using various methods to obtain data, that universities have experienced in recent years.

**Example of a serious data breach of personal data:**

**A University in the UK had a serious data breach when personal data was mistakenly published online. The data included names, addresses, dates of birth and even health information of students. It was initially uploaded to a microsite created by a student project and not taken down properly. The ICO fined the University £120,000 in 2018, one of the first significant penalties issued to a UK University for a data breach.**

**Source [ICO Enforcement Action, 2018]**

**A cyberattack led to a data breach involving student applicants' personal information.**

**Details:**

- **Personal data such as names, addresses, phone numbers, and email addresses of undergraduate applicants for 2019 and 2020 were stolen.**
- **Some students received fraudulent invoices as a result.**
- **The breach was linked to unauthorised access via a phishing attack.**
- **There is no public record of a fine being issued by the ICO in respect of this breach.**

**Source: [University Press Release, 2019]**

**A widespread ransomware attack hit multiple UK universities using the Blackbaud cloud platform.**

**Details:**

- **Affected institutions and universities across the UK**
- **The attackers stole donor and alumni data: names, contact details, and donation histories.**
- **Blackbaud paid the ransom, claiming the attackers destroyed the data afterward (a claim that drew criticism).**

**Source: [The Guardian, 2020]**

**Blackbaud's European subsidiary was reprimanded by the ICO under Article 58(2)(b) of the UK GDPR for failing to comply with Article 32 (security of processing) in relation to this incident. The ICO did not impose a fine for the Blackbaud breach.**

**St Mary's University College**

**Reporting a Data Breach**

1. If you know or suspect that a personal data breach has occurred, please report this breach using the link below to complete an online form https://forms.office.com/e/GX4f7s8pTM

2. Following a data breach, the Data Protection Officer will begin an investigation.
3. Using the information provided on the online form, the Data Protection Officer must assess the level of risk and if there is a requirement to proceed to notification.
4. The Data Protection Officer must inform the Director of Finance and Administration (or Principal in their absence) of the breach, prior to notifying the Information Commissioners Office.
5. Where agreed, the Data Protection Officer will notify the ICO within 72 hours of becoming aware of the breach, disclosing details of the incident as follows:
   - what has happened
   - when and how the College found out about the breach
   - the people that have been or may be affected by the breach
   - what action the College has taken as a result of the breach
   - who the ICO should contact if they require any further information.
6. In the event of a sufficiently serious data breach, the College will notify those affected without undue delay.
7. The Data Protection Officer will keep a detailed record of the breach including the facts surrounding it and remedial actions taken.
8. Conduct a review of data protection policies and procedures after managing the breach to identify any weaknesses that may have contributed to the breach.

**Definition of Personal Data Breach**

The GDPR defines a "personal data breach" as:

"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. It also means that 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

**Basic Security Considerations.**

The College must ensure that there are levels of protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. There is therefore essential to have systems in place that can identify when a breach has occurred. The expectation is that in the case of technology, there are ways of detecting unauthorised access. In the case of hard copy, departments must have a log of all documents held and regularly review these for retention and disposal purposes. Sensitive data must be stored securely and any breach of this must be reported immediately.

"A personal data breach may, if not addressed in an appropriate and timely manner, may result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

If you have any questions regarding this information, please contact:

Data Protection Officer
St Mary's University College
191 Falls Road
Belfast
BT12 6FE

028 9026 8320

St Mary's University College Belfast
A College of Queen's University

**To be completed by the Data Protection Officer**

| Risk to individual's privacy* | High/ Medium/ Low |
|---|---|

The following general descriptions are for review.

High – includes personal and sensitive data relating to a number of individuals

Medium – includes personal data but not sensitive data relating to a number of individuals

Low – there is an isolated incident with no risk to freedom or rights of individuals.

| Need to inform Data Subjects | Yes/ No |
|---|---|

Recommendations of College to Report Breach

Notify ICO

Do not notify ICO.

Signed: _____ Date: _____

Data Protection Officer

Signed: _____ Date: _____

SMT

St Mary's University College Belfast
A College of Queen's University

# Flowchart of Data Breach Reporting Process