

**Belfast Metropolitan College**

**Data Breach Incident Response Plan**

TABLE OF CONTENTS

[1. INTRODUCTION 3](#_Toc430329179)

[2. PURPOSE 3](#_Toc430329180)

[3. What is a PERSONAL Data Security Breach? 3](#_Toc430329181)

[4. What TYPES OF DATA do these procedures apply to? 4](#_Toc430329182)

[5. WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACHES? 4](#_Toc430329183)

[6. PROCEDURE FOR REPORTING DATA SECURITY BREACHES 4](#_Toc430329184)

[7. PROCEDURE FOR MANAGING DATA SECURITY BREACHES 5](#_Toc430329185)

[Step 1: Identification and initial assessment of the incident 5](#_Toc430329186)

[Step 2: Containment and Recovery 6](#_Toc430329187)

[Step 3: Risk Assessment 6](#_Toc430329188)

[Step 4: Notification 8](#_Toc430329189)

[Step 5: Evaluation and Response 9](#_Toc430329190)

[8. RELATED POLICIES AND PROCEDURES 9](#_Toc430329191)

[9. FURTHER HELP AND ADVICE 10](#_Toc430329192)

[APPENDIX 1 –DATA SECURITY BREACH REPORT FORM 11](#_Toc430329193)

[APPENDIX 2 –DATA SECURITY BREACH RESPONSE FLOWCHART 14](#_Toc430329194)

**KEY**

|  |  |
| --- | --- |
| **BMC** | **Belfast Metropolitan College** |
| **CCIO** | **Corporate Contracts and Information Officer** |
| **COO** | **Chief Operating Officer** |
| **DP** | **Data Protection Act** |
| **E&FM** | **Estates and Facilities Management** |
| **FOIA** | **Freedom of Information Act** |
| **ICO** | **Information Commissioners Office** |
| **IMG** | **Incident Management Group** |
| **IT/IS** | **Information Technology/Information Systems** |

# INTRODUCTION

Belfast Metropolitan College is responsible for the security, integrity and confidentiality of all the data it holds. The College is obliged under the Data Protection Act 1998 to keep personal data safe and secure and respond promptly and appropriately to any data security breaches. Although all staffhave a responsibility for the information they generate, manage, transmit and use in line with the Data Protection Act 1998. It is their contractual duty to secure personal and confidential data at all times. Any person who knows or suspects that a breach of data security has occurred should report the breach immediately according to this Incident Response Plan.

**It is vital we take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the college.**

# PURPOSE

The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data (defined below) held by the College. These procedures are a supplement to the College’s Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

# What is a PERSONAL Data Security Breach?

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the College in any format. Personal data security breaches can happen for a number of reasons, including:

* the disclosure of confidential data to unauthorised individuals;
* loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data e.g. PCs, USB, mobile phones; Laptops, disks etc.;
* loss or theft of paper records;
* inappropriate access controls allowing unauthorised use of information;
* suspected breach of the College’s IT security and Acceptable Use policies;
* attempts to gain unauthorised access to computer systems, e.g. hacking;
* records altered or deleted without authorisation from the data “owner” and in line with the FE Sector Retention & Disposal Schedule;
* viruses or other security attacks on IT equipment systems or networks;
* breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information;
* confidential information left unlocked in accessible areas;
* insecure disposal of confidential paper waste;
* leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
* publication of confidential data on the internet in error and accidental disclosure of passwords;
* inadequate de-commissioning of buildings; and
* misdirected emails or faxes containing identifiable personal, confidential or sensitive data.

# What TYPES OF DATA do these procedures apply to?

These procedures apply to:

* all personal data created or received by the College in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
* personal data held on all College IT systems managed centrally by IT/IS, and locally by individual Schools and Departments; and
* any other IT systems on which College data is held or processed.

# WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACHES?

Personal data security breaches are managed by the Corporate Contracts and Information Officer (CCIO) in conjunction with the Head of IT /IS (where appropriate), with ultimate responsibility resting with the Head of Finance.

**In emergency situations**, the College’s Executive Team will take over responsibility for managing the incident (see section 8 below).

# PROCEDURE FOR REPORTING DATA SECURITY BREACHES

**In the event of a breach of data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.**

**If a breach or potential or suspected data breach has been reported to you please report this immediately to the CCIO or your Head of Department if applicable.**

**The Head of Department/School must then:**

* **report the incident** **immediately to the Corporate Contracts and Information Officer (CCIO) Mrs Carol McFadden – contact details below:** 
  + **During office hours, phone 02890 265335 or extension 5335 (or ext 5413 if unavailable).**
  + **Outside of Office Hours, phone 07918726304**
* **complete the attached Data Security Breach Report Form and email it to the CCIO at cmcfadden@belfastmet.ac.uk as soon as possible.**

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

# PROCEDURE FOR MANAGING DATA SECURITY BREACHES

In line with best practice[[1]](#footnote-1), the five steps in the table overleaf should be followed in responding to a data security breach:

**Step 1: Identification and Initial Assessment**

**Step 2: Containment and Recovery**

**Step 3: Risk Assessment**

**Step 4: Notification**

**Step 5: Evaluation and Response**

# Step 1: Identification and initial assessment of the incident

If you are aware that a data security breach has occurred, please report it immediately to the **Corporate Contracts and Information Officer** or your line manager/Head of Department (if applicable). The CCIO will liaise with the appropriate /Head of Department. You should complete part 1 of the Data Security Breach Report Form and email it to the CCIO without delay. Part 1 of the Report Form will assist the CCIO in conducting an initial assessment of the incident by establishing:

* if a personal data security breach has taken place; if so:
* what personal data is involved in the breach;
* the cause of the breach;
* the extent of the breach (how many individuals are affected);
* the harms to affected individuals that could potentially be caused by the breach; and
* how the breach can be contained.

Following this initial assessment of the incident, the CCIO who will, in consultation with the Chief Operating Officer (CCO), appoint an appropriate Lead Investigator to investigate the incident (eg Head of IT/IS for IT-related incidents, the Head of Finance for loss of paper records, etc.) and will decide if it is also necessary to establish an Incident Management Group (IMG) made up of a group of relevant College stakeholders to oversee and assist with the investigation. Any records relating directly to an investigation will be retained by the Corporate Contracts and Information Officer.

The Lead Investigator, liaising with the CCIO and the appropriate Head of the area affected by the breach, will determine the **severity** of the incident using the reference to the table below and by completing part 2 of the Data Security Breach Report Form (ie we will decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to the Executive Team). The severity of the incident will be categorised on a scale of 1 to 6. Where incidents are rated 3 or above the Incident Management Group will report directly to the Executive Team.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rating** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **Reputation** | No significant reflection on any individual or body  Media interest very unlikely | Damage to an individual’s reputation.  Possible media interest (eg prominent member of the College involved) | Damage to a department’s reputation.  Some local or subject specific FE media interest that may not go public | Damage to a service’s reputation/Chair  man of GB or CE/DCE involved.  Low key local or FE media coverage | Damage to College’s reputation/  local media coverage. | Damage to College’s reputation/  national media coverage. | Monetary  Penalty  Imposed by  ICO |
| **Individuals potentially affected** | Minor breach of confidentiality.  Only a single individual affected | Potentially serious breach. Less than 5 people affected or risk assessed as low (eg files were encrypted) | Serious potential breach & risk assessed high (eg unencrypted sensitive/health records lost) Up to 20 people affected | Serious breach of confidentiality eg up to 100 people affected and/or identifiable or particularly sensitive ie redundancies,  restructuring | Serious breach with either particular sensitivity (eg sexual or mental health details, identifying information of vulnerable people), or up to 1000 people affected | Serious breach with potential for ID theft or over 1000 people affected | Restitution to injured parties  Other Liabilities  Additional  Security  Legal Costs |

# Step 2: Containment and Recovery

Once it has been established that a data breach has occurred, the College needs to take immediate and appropriate action to limit the breach.

The Lead Investigator, liaising with the Corporate Contracts and Information Officer and relevant College staff will:

* Establish who within the College needs to be made aware of the breach (e.g. IT/IS, E&FM, HR, Corporate Development) and inform them of what they are expected to do to contain the breach (eg isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc);
* Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data);
* Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of serious harm to individuals); and
* Where appropriate (e.g. in cases involving theft or other criminal activity), inform the police.

# Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant College stakeholders are required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided at Stage 1 on the Data Security Breach Report Form will assist with this stage.

The Lead Investigator and Corporate Contracts and Information Officer in conjunction with the Head of Department/School in which the incident occurred will review the incident report to:

* Assess the risks and consequences of the breach:
  + Risks for individuals:
    - * What are the potential adverse consequences for individuals?
      * How serious or substantial are these consequences?
      * How likely are they to happen?
  + Risks for the College:
    - * Strategic & Operational
      * Compliance/Legal
      * Financial
      * Reputational Continuity of Service Levels
* Consider what type of data is involved, how sensitive is it? Were there any protections such as encryption? What has happened to the data? If data has been stolen it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged this poses a different type and level of risk;
* Consider how many individuals’ personal data are affected by the breach. It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment;
* Consider the individuals whose data has been breached. Whether they are staff, students, or suppliers will to some extent determine the level of risk posed by the breach and therefore, the actions in attempting to mitigate those risks;
* Consider what harm can come to the affected individuals. Are there risks of physical safety or reputation, of financial loss or a combination?
* Consider if there are wider consequences to consider such as a loss of public confidence in an important service the college provides; and
* Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The Lead Investigator and CCIO will prepare an **incident report** setting out (where applicable):

* a summary of the security breach;
* the people involved in the security breach (such as staff members, students, contractors, external clients);
* details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
* how the breach occurred;
* actions taken to resolve the breach;
* impact of the security breach;
* unrealised, potential consequences of the security breach;
* possible courses of action to prevent a repetition of the security breach;
* side effects, if any, of those courses of action; and
* recommendations for future actions and improvements in data protection as relevant to the incident.

The incident report will then be furnished to the Chief Operating Officer and the Head of Department/ School affected by the breach. Heads of Department / School will request relevant staff to update the risk registers at the appropriate levels where necessary. Any significant risks will be reported to the Audit & Risk Committee and addressed through the College’s Risk Management Policy.

# Step 4: Notification

On the basis of the evaluation of risks and consequences, **the Lead Investigator** in consultation with the Corporate Contracts and Information Officer, and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the College. For example:

* the Police
* individuals (data subjects) affected by the breach
* the Information Commissioner’s Office
* other bodies such as Department for Employment and Learning
* the press/media
* the College’s insurers
* bank or credit card companies
* trade unions
* external legal advisers

As well as deciding **who** to notify, the Lead Investigator must consider:

* **What** is the message that needs to be put across?

In each case, the notification should include as a minimum:

* a description of how and when the breach occurred;
* what data was involved; and
* what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the Lead Investigator should give specific and clear advice on what steps they can take to protect themselves, what the College is willing to do to assist them and should provide details of how they can contact the College for further information (e.g. helpline, website).

* **How to communicate the message?**

What is the most appropriate method of notification (e.g. are there large numbers of people involved? Does the breach involve sensitive data? Is it necessary to write to each individual affected? Is it necessary to seek legal advice on the wording of the communication?).

* **Why are we notifying?**

Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

Although there is no legal requirement on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner’s Office (ICO) expects that serious breaches should be brought to their attention. Serious breaches are not defined but guidance is available on the ICO website under Data Protection principle 7 Data Security.

Any contact with the ICO should be made through the Corporate Contracts and Information Manager. Initial contact with the ICO should be made by the Corporate Contracts and Information Manager within **two working days** of becoming aware of the breach, outlining the circumstances surrounding the incident through submission of a “Security Breach Notification Form”. The ICO will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data. In cases where the decision is made by the Lead Investigator and Corporate Contracts and Information Manager not to report a breach, a brief summary of the incident with an explanation of the basis for not informing the ICO will be retained by the Corporate Contracts and Information Manager.

# Step 5: Evaluation and Response

Subsequent to a data security breach, the Lead Investigator and the Corporate Contracts and Information Officer in consultation with the relevant stakeholders in the College will conduct a review to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

The Lead Investigator will send a copy of all data security breach reports to the CCIO who will compile a central record of incidents. The CCIO will report on incidents to the Head of Corporate Development at least on a quarterly basis in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed.

For each **serious** incident, the Lead Investigator and Corporate Contracts and Information Officer will conduct a review and report to the Executive Team:

* What action needs to be taken to reduce the risk of future breaches and minimise their impact?
* Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
* If there are any weak points in security controls that need to be strengthened?
* If staff and users of services are aware of their responsibilities for information security and adequately trained?
* If additional investment is required to reduce exposure and if so what are the resource implications?

# RELATED POLICIES AND PROCEDURES

These procedures underpin the following College policies and procedures:

* Data Protection Policy

http://www.belfastmet.ac.uk/AboutUs/Corporate/DataProtection.aspx

* IT Acceptable Use Policy http://www.belfastmet.ac.uk/docs/AUP/IT%20Acceptable%20Usage%20Policy%20v1-0.pdf
* Records Management Policy <http://www.belfastmet.ac.uk/docs/AboutUs/FOI/Records%20Management%20Policy%20@%20Sept%202012.doc>
* BYOD – Bring Your Own Device
* Confidential Waste Procedures and Guidelines <http://intramet.belfastmet.int/support%20sections/Forms/AllItems.aspx?RootFolder=%2fSupport%20Sections%2fFinance%2fFinance%20Administration%2fConfidential%20Waste%20Collection%202015&FolderCTID=&View=%7b122E6CC8%2d8289%2d4159%2d9072%2dCB40FC7201D8%7d>
* FE Retention & Disposal Schedules <http://intramet.belfastmet.int/support%20sections/Forms/AllItems.aspx?RootFolder=%2fSupport%20Sections%2fFinance%2fFinance%20Administration%2fRecords%20Management&FolderCTID=&View=%7b122E6CC8%2d8289%2d4159%2d9072%2dCB40FC7201D8%7d>
* FOI Policy

http://www.belfastmet.int/AboutUs/Corporate/FreedomOfInformation.aspx

# FURTHER HELP AND ADVICE

For further information and advice about this procedure and about data protection matters, please contact:

Mrs Carol McFadden

Corporate Contracts and Information Officer

Building 1 Level 2, Room 4

Belfast Metropolitan College

Millfield

Phone: 02890 265335 (or ext 5335)

Email: [cmcfadden@belfastmet.ac.uk](mailto:cmcfadden@belfastmet.ac.uk)

# APPENDIX 1 –DATA SECURITY BREACH REPORT FORM

**Please act promptly to report any data security breaches. If you discover a data security breach, please notify your Head of Department/School immediately. Heads of Department/School should complete Section 1 of this form and email it to the Corporate Contracts and Information Manager at** cmcfadden@belfastmet.ac.uk

|  |  |
| --- | --- |
| **Section 1: Notification of Data Security Breach** | **To be completed by Head of Dept/School of person reporting incident** |
| **Date incident was discovered:** |  |
| **Date(s) of incident:** |  |
| **Place of incident:** |  |
| **Name of person reporting incident:** |  |
| **Contact details of person reporting incident (email address, telephone number):** |  |
| **Brief description of incident or details of the information lost:** |  |
| **Number of Data Subjects 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 College use** | |
| **Received by:** |  |
| **On (date):** |  |
| **Forwarded for action to:** |  |
| **On (date):** |  |

|  |  |
| --- | --- |
| **Section 2: Assessment of Severity** | **To be completed by Lead Investigator in consultation with the Head of area affected by the breach and CCIO** |
| **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? |  |
| How many data subjects are affected? |  |
| 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   * **Sensitive personal data** (as defined in the Data Protection Act) relating to a living, identifiable individual’s  1. racial or ethnic origin; 2. political opinions or religious or philosophical beliefs; 3. membership of a trade union; 4. physical or mental health or condition or sexual life; 5. commission or alleged commission of any offence, or 6. 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 and 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 discipline or sensitive negotiations which could adversely affect individuals. |  |
| * Security information that would compromise the safety of individuals if disclosed. |  |
| **Category of incident (0-6):** |  |
| **Reported to Corporate Contracts and Information Manager on:** |  |
| If level 3 or above, date escalated by Lead Investigator to the College Executive Team |  |

|  |  |
| --- | --- |
| **Section 3: Action taken** | **To be completed by Corporate Contracts and Information Officer** |
| **Incident number** | **e.g. DB/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 Information Corporate Contracts and Information Officer on (date):** |  |
| **Reported to other internal stakeholders (details, dates):** |  |
| **For use of Information Corporate Contracts and Information 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:** |

# APPENDIX 2 –DATA SECURITY BREACH RESPONSE FLOWCHART

**Actual/potential/suspected breach of personal data identified**

Yes

Is it out of hours?

No (it’s Level 1 or 2)

Notify Chief Operating Officer and involve Executive Team, following Data Breach Mgt procedure

**Lead Investigator and Corporate Contracts and Information Officer to assess severity of incident & complete part 2 of Incident Report Form: Could this be a major incident?**

Yes (it’s level 3 or above)

Monitor and review

Assess risks and consequences

Is it a potentially serious incident?

Yes

**Breach to be reported to Head of Department/School**

No

Head to notify Corporate Contracts and Information Officer (02890 265335) & complete part 1 of Incident Report Form and email - cmcfadden@belfastmet.ac.uk

Corporate Contracts and Information Officer and Head of Finance to assess nature of incident and nominate a Lead Investigator

Write incident report

Commence notification process (if appropriate)

Head of Finance to contact Chief Operating Officer

No

Contact Corporate Contracts and Information Officer asap during working hours

Head of Finance (phone 07918726304)

Chief Operating Officer to decide if immediate action required

Contain the breach

Manage incident according to data breach mgt. procedure

Notify relevant BMC staff/managers

Report any significant findings to the ICO and relevant Audit & Risk Committee /Functional Area to prevent recurrence of breach

No

Yes

Chief Operating Officer to assess severity of incident and take appropriate action

1. UK Information Commissioner’s Office’s *‘Guidance on Data Security Breach Management’* [↑](#footnote-ref-1)