Data Security Breach Management SOP

SOP Number:
112-04-2014

Academic Year:
2024/2025 Onwards

Date Of This Issue:
April 2025

Responsible Owner and Enquiries:
Records Manager

Summary of Contents

In compliance with legislation and in line with the College Data Protection Policy this Standard Operating Procedure (SOP) provides staff with guidance in relation to actions they must take if they discover or suspect a breach in data security and the procedures which will be followed to contain, rectify and evaluate the breach.

Review Information (Responsible Owner):

First Created:	May 2013
Last Reviewed:	April 2025
Next Review:	May 2026

Change Type at last Review:
~~No~~/Minor/~~Significant~~ (delete as appropriate)

Approval/Noting By:
CMT: 17 April 2025

Previous Reference (for control purposes):
029-06-2013

Date of Last Accessibility Screening:
June 2024

Contents

1.0 Change History

Changes to this SOP are documented in Appendix 1 of this document. When reading electronic copies of this document, you can click here to view the change history.

2.0 Background

As a Data Controller the College must obtain, manage, process, and store all data in compliance with the General Data Protection Regulations (UK GDPR) and its 6 main principles as per Article 5.

Article 5(f) of the UK GDPR states personal data must be:

‘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')’

Processing is defined in Article 4(2) as:

“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”

The College holds a large amount of data / information, both in hard and electronic copy. This includes personal or confidential information (about people), and non-personal information which could be sensitive or commercial, for instance financial data.

This procedure sets out the process to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the College.

A data breach is defined in Article 4(12) as:

“breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”

As the Data Controller, the College is accountable for all data being processed as part of the organisational function. It is therefore imperative that a confirmed or suspected breach is reported as soon as possible. Failure to report a breach may result in damage and distress to both the individuals concerned and the College reputation and physical/electronic facilities.

Failure to report a breach also contravenes Article 33 of UK GDPR which states:

‘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 regular Data Protection training and approved policies and procedures to assist its staff in minimising the risk of theft, unauthorised access, loss and damage while fulfilling their contracted duties.

3.0 Scope

Section 4 of this Standard Operating Procedure applies to College staff and authorised third parties which can include temporary staff and work experience candidates.

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 and/or Data Incident Response Team.

Section 5 of this Standard Operating Procedure applies to the DPO and Incident Response Team.

4.0 Data Breach Procedures (All staff)

4.1 Recognising a Potential Data Breach

It is important for all staff to be able to recognise a potential data breach or an event which has resulted in personal information being compromised.

An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the College's information assets and/or reputation.

An incident includes but is not restricted 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 stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Sending personal data to an incorrect recipient
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- Unsecure disposal of paper records containing personal data

If a data security breach occurs, the College will respond to and manage the breach effectively by means of a 5-part process.

- Reporting a Breach
- Containment and Recovery
- Assessing the Risks

- Notification of Breaches
- Evaluation and Response

4.2 Reporting a Potential Breach

Article 33 of GDPR requires the College to notify the ICO of reportable breaches within 72 hours of if it being discovered. In some cases, the ICO should also be informed of suspected breaches, if significant.

It is therefore critical that once any member of staff or authorised third party have knowledge of a breach or suspect a breach has occurred, they must contact the DPO immediately.

Delays in reporting to the ICO must be accompanied with and explanation of reasons for the delay. The College DPO contact details are:

Data Protection Officer
SERC
Bangor Campus
Castle Park Road
Bangor
BT20 4TD
informationrights@serc.ac.uk

Should the DPO be unavailable, please contact a member of CMT.

All known details should be included in the initial reporting of the incident.

The immediate response will be to establish the nature of the breach and the data involved e.g. has personal data been compromised, what type of personal data and how many individuals may be affected. This will determine which Head of Department will be nominated as the Lead Investigator, the nominee must be notified.

The DPO must report all breaches to the Principal and Chief Executive/College Management Team through agreed internal communications.

The following details of a suspect or confirmed data breach must be recorded in the College register/log:

- Date of Incident
- Time of Incident
- Who Reported Breach
- Due Date of Notification
- Description of Incident/Breach
- Does this incident/breach involve personal data?
- Type of Incident
- Number of people affected?
- Nature of breach
- Description of data
- Sensitive Information

- Category of Sensitive Information
- Risk Rating
- Consequences of breach
- Have all clients and staff informed?
- Remedial action taken?
- All Regulators informed?
- ICO Notification Date
- Media Informed
- Case Closed Date
- Further Action

4.3 Report Regarding Individuals Own Data

Should an individual have a concern regarding the processing their own data e.g., suspected unauthorised access or disclosure, they should raise this with the DPO in the first instance.

The DPO may be able to put the individual at ease if the concern can be resolved by immediate explanation e.g., the processing is a statutory obligation.

Should the report warrant further consideration, the DPO will conduct an investigation within a timeframe agreed by both parties.

The DPO/nominee will assume the role of Lead Investigator and engage with all relevant parties to gather evidence, evaluate, and report the findings.

If the evidence indicates the allegation to be unfounded, the individual who made the report will be notified of this and a short report made for records which will be retained by the DPO.

If the evidence supports the allegation, the DPO will issue the final report and supporting evidence to the appropriate Head of Department and HR. In addition, the DPO, with reference to Section 5.7.3 of this SOP, will assess the appropriate actions to be taken e.g. Report to the ICO.

4.4 Containment and Recovery

Once details of the breach are known, the DPO will liaise with relevant personnel to contain the effect of the breach. This may include personnel from ICT, Human Resources, College Management Team, and Estates and on some occasions, external suppliers.

The DPO and the department specialists will agree what action must be taken to limit the damage caused by the breach and if possible, restore any lost data e.g. backup tapes. Priority actions may include password changes, disabling swipe access to secure areas within the buildings or searching for lost equipment.

4.5 Assessing the Risks

Once the breach has been contained, the DPO and department specialists will assess risks associated with the loss of the data.

See local Data Breach Incident Response Plans for risk scoring.

4.6 Notification of Breaches

Where data loss has been confirmed and the risk has been assessed as high, the College is obliged to notify parties affected by the breach.

4.6.1 Notifying the individuals

The DPO and department specialists will establish the identities of individuals whose personal data has been compromised and agree the correspondence to be sent to each subject.

The correspondence should include:

- how and when the breach occurred.
- what data is involved?
- actions taken by the College.
- advice in relation to what steps the individual may need to take to protect themselves in light of their data being compromised e.g. changing a password, cancelling a credit card.
- has the Information Commissioners Office (ICO) been informed.
- contact name, website link if they need further information in relation to the incident.

4.6.2 Notifying the Information Commissioners Office (ICO)

The ICO must be notified of all breaches where large numbers of individuals are involved or where the consequences are serious within 72 hours – the DPO will be responsible for this correspondence.

As per Article 33.2 of GDPR, when notifying the ICO, the information should include, at minimum:

- 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.
- name and contact details of the data protection officer or other contact point where more information can be obtained.
- describe the likely consequences of the personal data breach.
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The ICO will not normally inform the media of a breach however they may advise the College to inform the media of the breach.

4.6.3 Notifying the Media

Should the ICO advise that the media is informed of the data breach, the DPO will liaise with the Principal and Chief Executive to agree a statement which will be released to the press via the College's Communications and Marketing department, containing all relevant information pertaining to the incident.

4.7 Evaluation and Response

While it is critical to contain and assess the risks of a breach, the College must evaluate events leading to the breach and the effectiveness of its response to it.

While carrying out an evaluation the DPO will convene with department specialists, a member of CMT and if necessary, seek advice from the ICO regarding what measures the College should and can take to avoid a breach of a similar nature in the future. The College Record of Information Processing should be used a point of reference at this stage.

Considerations should be given to the following:

- Was the breach a result of inadequate policies or procedures?
- Was the breach a result of inappropriate training?
- Where are documents stored?
- Who has access rights to what data?
- Has this breach identified potential weaknesses in other areas?
- Security of electronic information assets.

4.8 ICO Response

The ICO will evaluate the data breach and carry out their own investigation into the surrounding circumstances, the nature and seriousness of the breach, and the adequacy of any remedial action taken by the College will be assessed and a course of action determined.

The ICO may:

- Record the breach and take no further action, or
- Investigate the circumstances of the breach and any remedial action, which could lead to one of the following:
    - no further action.
    - a requirement on the data controller to undertake a course of action to prevent further breaches.
    - formal enforcement action turning such a requirement into a legal obligation.
    - where there is evidence of a serious breach of the GDPR, whether deliberate or negligent, the serving of a monetary penalty notice requiring the organisation to pay a monetary penalty of an amount determined by the Commissioner up to the value of €20m or 4% of global annual turnover.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

5.0 Incident Response Team Procedures

5.1 Introduction

The General Data Protection Regulations (GDPR) and Data Protection Act (2018) place obligations on the College to have in place, organisational and technical measure to demonstrate processing of personal data is performed in accordance with legislation.

In the event of a suspected or confirmed security incident it is critical that the College quickly establishes whether a personal data breach has occurred and, if so, promptly take steps to address it and notify all relevant parties.

5.2 Purpose

The purpose of this SOP is to provide the Data Protection Officer and Incident Response Team with an effective and detailed response plan in the event of a suspected or known data breach being reported.

This SOP is primarily for the Incident Team which will be agreed to conduct an investigation.

Staff not named in the Incident Team should refer to the Data Security Breach Management SOP.

In the event of a major incident, the Business Continuity Plan will become operational in the first instance and this SOP referred to for College's data protection obligations.

5.3 Confidentiality

It is important that the College/Incident Team is given time and privacy to examine thoroughly and conclude any investigation without unnecessary and distracting interference. The College will actively communicate key information as appropriate both during and post investigation.

Personnel/PA's involved in the implementation of this SOP and communications in the event of an incident, must maintain the strictest confidence in relation to details made known to them throughout the process. Disclosure will be on a necessary basis only.

Unauthorised disclosure of details may prejudice the investigation and increase information risk if the incident is founded.

5.4 Scope and Responsibilities

For the purpose of this procedure, data security breaches include both confirmed and suspected incidents.

This procedure relates to all 'Personal' and 'Special Category' data held by the College regardless of format.

This document applies to the Data Protection Officer, College Management Team, key information managers (IT, HR, Knowledge Management) and authorised staff whose role/expertise is required to fully contain, investigate and manage a breach of personal data.

The objective of this procedure is to identify and contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

It is critical the College key decision makers familiarise themselves with this SOP and provide the necessary leadership, backing and resources to properly develop and implement this plan. This will also create a clear and transparent line of communication to the Governing Body, DfE and other stakeholders such as investors.

5.5 College Management Team

- Responsible for overseeing and directing the incident response and ensuring that staff have followed this procedure.
- For significant data breaches, CMT will appoint relevant personnel, including Lead Investigating Officer to the Incident Team to manage and investigate the data breach.
- Ensure that all relevant information and appropriate resources are provided as soon as is practicable to support the breach investigation process.
- Responsible for providing all professional advice in relation to the management of communications in relation to any data breach and for managing all internal and external communications.
- Reporting data breaches to the Governing Body, Department for the Economy (DfE) and other relevant third parties where necessary e.g. PSNI.

5.6 Incident Team

- This team will include personnel deemed relevant and necessary to manage the following elements of the breach:
  - Containment and recovery
  - Assessing the risks
  - Notification of breaches
  - Evaluation and response
- Responsible for ensuring that all appropriate support and technical expertise is provided to the Data Protection Officer in order that they can determine the nature and severity of the breach and provide advice to the College on their legal responsibilities in relation to breach reporting etc.
- The Incident Team will consist of as a minimum, Principal and Chief Executive, Deputy Chief Executive, Head of Finance (for purposes of audit), Data Protection Officer, Head of Department/School relevant to the incident.
- If the incident relates to College IT systems and networks, IT personnel will be responsible for providing all professional and technical support and risk analysis in relation to the management and containment of any breach.
- Agree accuracy of detail in communications to be issued to data subjects and relevant parties.

5.6.1 Information and Cyber Security Committee

Chaired by the Deputy Chief Executive (SIRO), this committee is responsible for considering the outcome of the data breach report and considering what measures the College can take to prevent a recurrence of the incident. This may include recommendation of new resources, training or Policy/SOP implementation.

5.6.2 Data Protection Officer

- Responsible for ensuring that any reported breach is investigated and for ensuring that these procedures are followed.
- Responsible for reporting all data breaches to the Principal and Chief Executive/College Management Team.

- Responsible for providing legal and data management advice in relation to the operation of these procedures.
- Responsible for liaison with the Information Commissioner's Office (ICO) and for reporting the breach, where required.
- Responsible for determining the nature and severity of the breach and providing advice to the College on their legal responsibilities in relation to breach reporting etc.

5.6.3 Communications and Marketing

- Responsible for developing a public statement for release either pro-actively or in response to media enquiries.
- Track and analyse media coverage and determine if a response is necessary.
- Advise if public information via the College website is appropriate based on the nature of the incident.

5.6.4 All Staff

- All staff have a responsibility for reporting a known or suspected data breach and information security incidents immediately.
- All staff should report the matter to their line manager and the Data Protection Officer.

5.7 Incident Management

5.7.1 Identifying an incident

It is critical all staff are familiar with the Data Security Breach Management SOP and have completed all mandatory training to understand their role in the event of a breach of data security.

Data breaches can be identified via a number of different channels, for instance:

- Data Processor makes the College aware of an incident where SERC data has been compromised.
- Automated system monitoring - detecting a potential data breach/unusual activity.
- End users may report breaches/suspicion to the IT personnel, however, be aware that issues reported in this way may not be logged as breaches.
- After details are published by the hackers, or when members of the public find IT equipment/files and report it to news outlets. On occasions it may be that the breach is in the public domain before the organisation learns of it. Containment of the breach will be more difficult in this scenario.
- A one-off event which destroys hardcopy information e.g. fire/flood/explosion and risk to records is immediately obvious.
- Whistleblowing facilities for groups such as staff, customers and suppliers to report concerns anonymously.

5.7.2 Reporting an incident

Any individual (staff or student) who accesses, uses or manages the College's information is responsible for reporting suspected or known data breach and information security incidents to the Data Protection Officer immediately as per the Data Security Breach Management SOP:

Any individual (staff or student) who accesses, uses or manages the College's information is responsible for reporting suspected or known data breach and information security incidents to the Data Protection Officer **immediately** as per the Data Security Breach Management SOP:

Table 1: DPO Contact Details

Name	Contact Details
Data Protection Officer	informationrights@serc.ac.uk 02891 276603

The DPO will notify the Principal and Chief Executive/CMT.

In the absence of the Data Protection Officer, Directors/key data custodians should be contacted for advice:

Table 2: Other Key Contacts

Name	Contact Details
Principal and Chief Executive	kwebb@serc.ac.uk 07801 082387
Deputy Chief Executive	tmartin@serc.ac.uk 07500 667292
Deputy Principal Student Support Services	hmckee@serc.ac.uk 07825 146992
Deputy Principal Curriculum	gritchie@serc.ac.uk 07867 423102
Head of Human Resources	ecarson@serc.ac.uk 07876 195813
Head of Finance	dwmccullough@serc.ac.uk 07799 473579
Head of Training Programmes and Apprenticeships	vboyd@serc.ac.uk 07826 521798
Chief Technology Officer	aemmett@serc.ac.uk 07899 958209
Head of Knowledge Management	cfrancis@serc.ac.uk 07990 515379

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

The incident report must include full and accurate details of the incident, including a minimum of when the breach occurred (dates and times), who is reporting it, if the data relates to personal data, the nature of the information, and how many individuals are involved.

Consideration must be given to contacting the College legal representation for Information Governance.

If in the early stages the data breach is in relation to criminal activity, the PSNI must be notified without delay.

5.7.3 Initial Assessment of the Incident

The DPO and relevant senior manager will undertake an initial assessment to determine if the incident is one of the following:

- Data Breach (personal data)
- Near Miss
- Formal Complaint
- Other

With reference to the information provided in the initial report, they will also determine:

- who is the Data Controller?
- is the breach still occurring?
- what immediate action can be taken to reduce further compromise (e.g., enforced password change, deactivate staff passes, re-locate records, remote wipe of devices)

The three incident weighting tables below should be used at this point to calculate the level of risk posed based on known information, and whether the incident should be treated Minimum, Moderate or Severe according to the Incident Scoring Matrix.

Table 3: Incident Weightings Step 1 - Scale

Number of Data Subjects	Score
1-10	1
11-100	2
101-1000	3
1001+	4

Table 4: Incident Weightings Step 2 - Data Types

Data Types Involved	Score
No special category data	Reduce score by 1
Information already accessible or in public domain	Reduce score by 1
Low level of harm to individual	Reduce score by 1

Table 5: Incident Weightings Step 3 - Additional Factors

Additional Factors	Score
Detailed information at risk	Increase score by 1
High risk confidential information (i.e., National Insurance, Passport, Driving Licence and, Bank Details)	Increase score by 1
One or more previous similar incidents in the last 12 months	Increase score by 1
Failure to implement, enforce or follow technical safeguards to protect information	Increase score by 1
The PSNI have been notified	Increase score by 1
Existence of factors cited in Recital 75 of the UK GDPR.	Increase score by 1
Individuals are at risk of physical harm	Increase score by 2
Special Category Data	Increase score by 3

Table 6: Incident Scoring Matrix

Scores	Risk Rating	Notification
0-4	Minimal	• Recorded internally as a data breach • Not reported to ICO • Report to Information and Cyber Security Committee • Reported to CMT through quarterly risk report
5-7	Moderate	• Recorded internally as a data breach • Data subjects should be notified • Report to Information and Cyber Security Committee • CMT aware via Incident Team • Consideration should be given to reporting to ICO (72-hour timescale applies) • Should be reported to Governing Body at next meeting • Prepare press statement
8+	Severe	• Recorded internally • Must be reported to ICO within 72 hours • Data subjects must be notified • Report to Information and Cyber Security Committee • CMT aware via Incident Team • Report to Governing Body • Report to DfE • Prepare press statement

5.7.4 Establish Incident Team

Moderate/Severe or ongoing breaches will require the immediate appointment of an Incident Team and the appropriate steps will be taken immediately to minimise the effect of the breach.

The Incident Team need to be called together as soon as the data breach is known. Initially the meeting may be via Microsoft Teams; however meeting in person within the initial days may be beneficial. An initial meeting should be held with the response team to establish the next steps and who to involve at that stage along with:

- Identification of a Lead Investigation Officer (LIO).
- The value of the data which has been compromised needs to be understood so that the recovery can be prioritised. This may depend not only on the volume of data but the nature of data (for example personal sensitive data as defined by GDPR)
- A decision on record keeping – both relating to organisational logs and records that the team create during the response. It is good practice to note down the timing of events, such as when incident identified, by who, immediate response, dates individuals were informed (e.g. data subjects, Senior Management, DfE, ICO, PSNI), advice from legal team, when decisions were made and who was involved in making them, nature of enquiries from data subjects including Data Subject Rights requests e.g Access, Erasure.
- A review of whether affected individuals need to be informed. The information that needs to be provided to them and advice to help them protect themselves from its effects (See Section 5.7.7)

- A review of whether external bodies e.g. Data Controllers, regulators need to be involved and initiate this, using the appropriate process and within laid down timescales (ie ICO within 72 hours of becoming aware of it).
- Whether a forensic expert is needed to understand what needs to be searched for, collect any/all items related to the incident as well as deciding whether the police, etc. need to be informed. Such contacts should be authorised by a member of CMT.
- Ensuring any internal investigation is kept as confidential as possible; not only to protect the data but also to prevent prejudicing the investigation.
- Work to prevent any further breach and stop the current breach (if it's ongoing) and mitigate the damage that the breach, and any leaked data, can cause. This might include the Marketing and Communications department and the issuing of press statements. Ensure that the response team contains people with the authority to initiate this.
- Consider developing website information e.g. FAQ's
- Beginning to investigate the cause of the incident. This may take a lower priority whilst the team 'firefight' initially, but establishing how it happened may assist with stopping the current breach.
- How to recover systems in line with contracts/SLAs. This may involve invoking the Business Continuity Management Plan if key systems are unusable.
- Establish who should be informed, both internally and externally; this could include IT, HR, Estates, legal team, Governing body, DfE, internal audit, media outlets, regulators, PSNI, insurers, alarm company and so on. (See Section 5.7.7)
- Consider the establishment of a Helpdesk with contact numbers agreed for data subjects to contact if notifications are to be made.
- Where the College is acting as Data Processor, the Data Controller should be contacted, advising the information owner that data they are responsible for has been breached.
- Being aware of false alerts.

A central repository (e.g., Microsoft Teams) for all evidential documentation should be created with access only permitted to the Incident Team.

5.7.5 Containment and Recovery

The breach may affect more than one physical or virtual site and all staff selected as per procedures outlined in Section 5.6 will need to have the relevant permissions to make decisions or enforce actions on these sites.

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

Advice from the Incident Team and key data custodians should be sought in resolving the incident promptly.

5.7.6 Investigation and Risk Assessment

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

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- Who are the individuals whose data has been compromised? E.g. students, applicants, staff, customers, clients or suppliers.
- How many individuals' personal data is affected by the breach?
- What type and volume of personal data is involved?
- How sensitive is the data? "Sensitive personal data" and also sensitive information such as bank account details due to the risk of fraud
- What has happened to the data? Has it been lost, stolen or damaged? If the data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate. If the data has been damaged, this poses a different type and level of risk.
- If the data was lost/stolen, were there any protections in place to prevent access/misuse? E.g. Two-Factor Authentication, encryption of data/device.
- If the data was damaged/corrupted/lost, were there protections in place to mitigate the impact of the loss? E.g. back-up tapes/copies.
- What could the data tell a third party about the individual? Could it be misused? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- Is there actual/potential harm that could come to any individuals? E.g. are there risks to: physical safety; emotional wellbeing; reputation; finances; identity theft theft/fraud from release of non-public identifiers); or a combination of these and other private aspects of their life?
- Are there wider consequences to consider? E.g. Loss of public confidence in an important service provided by the College?
- Are there others who might advise on risks/courses of action? E.g. if individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help prevent fraudulent use
- Are there existing policies/SOPs which detail how this data should be processed.
- Which GDPR Principals have been implicated? E.g. Accuracy, data limitation

The Risk Table in Section 5.7.3 will give the incident a score, the score will then determine the overall risk status and an indication of the notifications which should be prepared for and completed.

5.7.7 Notifications

Notifying the Information Commissioners Office

When a personal data breach has occurred, the College must quickly establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then you must notify the ICO; if it is unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it’s important to focus on the potential negative consequences for individuals. The ICO will only be notified if personal data is involved.

The LIO and / or the DPO, in consultation with the Principal and Chief Executive/nominee, will determine who needs to be notified of the breach. Ultimately the DPO must score and decide whether the ICO should be notified of the breach.

More detailed guidance on when and how to notify ICO is available from the ICO website. For reporting the DPO must complete the standard form https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

The ICO recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. There is an allowance to provide the required information in phases, as long as this is done without undue further delay.

To meet this allowance, the College must prioritise the investigation, give it adequate resources, and expedite it urgently. If the College knows within this timeframe it will be unable to provide full details within 72 hours, it is a good idea to explain the delay and tell the ICO when you expect to submit more information. The initial report must be made within he 72 hours. Do not wait until all information has been gathered.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Would notification help the College meet its obligations under the seventh data protection principle;
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

The LIO and or the DPO must also consider notifying third parties such as the police, insurers, bank 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.

All actions will be recorded by the Incident Team on the Timeline document.

Notification to the individuals whose personal data has been affected by the incident will include a description of how 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 an appropriate named contact officer in the College who they can contact for further information or support in relation to what has occurred.

Notification to individuals whose personal data may have been affected by the breach

When should data subjects be notified of the breach?

- If a breach is likely to result in a high risk to the rights and freedoms of individuals, the law says that the College must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.
- A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. Again, the College needs to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

What information should be provided to individuals when telling them about a breach?

Communications must describe, in clear and plain language, the nature of the personal data breach and, at as a minimum:

the name and contact details of the College Data Protection Officer or other contact point where more information can be obtained e.g. helpline number, email address, website links

- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken by the College, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.
- Advise on extra measures the individuals may wish to take as an added layer of protection.

5.7.8 Evaluation and Response

Once the initial incident is contained, the Incident Team 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 review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- 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 CMT and in more serious cases it may be appropriate to report to the College Governing Body.
- Whether there are wider consequences to the breach

6.0 Communication Plan

This Procedure will be uploaded to the College intranet and referred to in staff induction and training.

7.0 Review

This procedure will be reviewed annually, or when the need for change has been identified.

Appendix 1: Document Change History

Version	Date	Change Detail
1.0	03/06/2024	Moved to new Accessibility template
1.1	03/06/2024	Updated Key Roles & Contacts in Section 5.7.2 to reflect restructuring Changes. Minor formatting and reference changes across document
1.2	April 2025	Review period changed to “annually” – no other changes necessary

Appendix 2: Examples of Incidents Which Should Be Reported (Step 1- Report)

Use the Incident Report Form in appendix 1 for the following types of incidents or similar. If in doubt, report it.

Human error

- Personal data emailed, posted or handed to the wrong recipient
- Excessive/non-essential personal data provided to otherwise valid recipients
- Personal data received in error
- Loss of hard copy material containing personal data
- Loss of any College-owned* data storage device, regardless of the data it contains, e.g. laptop, PC, USB drive, tablet, removable hard drive, smart phone or other portable device
- Unauthorised publication of personal data onto a website or social media channel

Theft

- Theft of hard copy material containing personal data
- Theft of any College-owned* data storage device, regardless of the data it contains e.g. laptop, PC, USB drive, tablet, removable hard drive, smart phone or other portable device

**Loss or theft of any privately-owned devices must be reported if they contain personal data related to SERC activities.*

Malicious intent

- Attempts (either failed or successful) to gain unauthorised access to SERC systems, e.g. hacking
- Virus or other malicious malware attacks (suspected or actual)
- Compromised user accounts, e.g. disclosure of user login details through phishing
- Information obtained by deception ("blagging")
- Deliberate leaking of personal data

Malfunctions

- Failure of software or hardware leading to personal data loss
- Damage or loss of personal data due to fire, flood, power surge or other physical damage

Appendix 3: Initial Assessment, Containment and Recovery Checklist

Step	Posible Actions
1. Identify LIO and response team as required	• LIO to take the lead in investigating the extent and nature of the breach, and to contact and co-ordinate with the 'Incident Team' members as necessary. Other staff groups may be required to provide expertise and support: • Responsible Staff Members • External Relations/Internal Communications • Estates • HR • Legal
2. Ensure that any possibility of further data loss is removed or mitigated as far as possible.	• Change passwords or access codes • Isolate/close part of network • Take down webpages • Restrict access to systems to a small number of staff until more is known about the incident • Inform building security so appropriate additional physical measures can temporarily be put in place
3. Determine whether anything can be done to recover any losses	• Physical recovery of lost data/equipment – inform security/check relevant lost property offices • Physical recovery of stolen data/equipment – inform security and the police as appropriate • Use back-ups to recover corrupted data • Recall incorrectly sent emails. If the recall is unsuccessful try contacting the person(s) to whom the data has been disclosed, apologise and ask them to delete the email from their systems (including from deleted items folders) and to confirm that they have done so • Retrieve paper documents from any unintended recipients
4. Ensure all key actions and decisions are logged and recorded on the Data Breach Timeline	• Complete the Data Breach Timeline at each stage of the process to keep an evidence and audit trail of the breach and the remedial action taken. This will be important for evaluation and for demonstrating compliance to the Information Commissioner's Office

Appendix 4: Notification Requirements Checklist

Notification can be an important part of the breach management process, but notification must have a clear purpose.

- Are there any legal, contractual or regulatory requirements to notify?
  e.g. terms of funding; contractual obligations.
- Can notification help the College meet its security obligations under data protection legislation? E.g. prevent any unauthorised access, use or damage to the information or loss of it.
- Can notification help the individual? Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their accounts)?
- If there is a high risk to individuals, there is a legal requirement to notify those individuals without undue delay. The requirement to notify individuals does not apply if:
  - the personal data concerned was protected with appropriate technical and organisation measures (e.g. encryption);
  - the College has taken steps which ensure 'high risk' unlikely to materialise (e.g. lost data has been retrieved or compromised passwords reset); or
  - it would involve disproportionate effort a public communication or similar may be required as an alternative depending on the risk)
  - external relations/internal communications as appropriate
- If there is a risk to individuals, there is a legal requirement to notify the Information Commissioner's Office without undue delay and (where feasible) within 72 hours of becoming aware of the breach.
- Consider the dangers of over- notifying. E.g. notifying 5000 students of an issue affecting only 50 students may well cause unnecessary concern and a disproportionate number of enquiries.
- Consider who should be notified, what you will tell them and how you will communicate the message. There are several different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. Consider how notification can be made appropriate for different groups of individuals (e.g. children, staff, students, customers). Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done and/or what will be done to respond to the risks posed by the breach.
- When notifying individuals, give specific and clear advice on the steps they can take to protect themselves and what the College is willing to do to help them.
- Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or FAQs on a web page). Also include contact details for the College's Data Protection Officer.
- Consider the need to notify any third parties who can assist in helping or mitigating the impact on individuals e.g. police, lost property offices, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

Appendix 5: Example Notification to Data Subject

Dear xxxxxxxxxx,

Notification of a personal data breach

We are sorry to inform you of the discovery of a breach of security which may have resulted in the potential unauthorised disclosure of your personal data to an unknown third party.

The breach was discovered on xx/date/xx as a result of normal operation of controls regarding suspicious email activity.

As a result of our initial investigation of the breach, we have concluded that the following categories of information may be affected:

- xxxxxxxxxxxxx
- xxxxxxxxxxxxx

We understand this notification may cause you concern and we would like to reassure you that all possible steps are being taken to investigate the factors surrounding this incident. All possible actions have been taken to secure data and prevent any further access.

What we are doing

- SERC has informed the Information Commissioners Office of this breach.
- SERC has reported the incident to the PSNI Cyber Crime Unit
- xxxxx offer of service to protect their information xxxxx
- SERC has established a dedicated helpdesk to assist with any questions about the incident. The helpdesk is available from xxxtimexxx (xxxdaysxxx). The contact details are as follows:
    - Email dataprotection@serc.ac.uk
    - Telephone (028) 91xx xxxx.

We recommend that you take precautionary measures to xxx e.g. monitor your bank statements for evidence of fraud or identity theft. If you are concerned or notice any suspicious activity on your bank account, you should contact your bank(s).xxx

The Data Protection Officer details are as follows:

Name: Siân Harvey

Address: SERC, Castle Park Road
Bangor
BT20 4TD

Email: informationrights@serc.ac.uk

The College understands the importance of your personal information. We take the protection of that information very seriously and we are sorry to have to write to you in these circumstances.

Yours sincerely,

[Name, job title, contact details]

Appendix 6: Evaluation and Response Checklist

- Establish where any present or future risks lie.
- Consider the data and contexts involved e.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
- Consider and identify any weak points in existing security measures and procedures e.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
- Consider and identify any weak points in levels of security awareness/training. Fill any gaps through training or tailored advice.
- Report on findings and implement recommendations to the Cyber Security and Information Committee, other relevant staff members, the Audit and Risk Committee and SLT where appropriate.