Procedure 1095 – Data Breach Reporting Procedure

Introduction

As a college we hold, process and share personal data for many purposes. Every care is taken to protect this personal information from accidental or deliberate misuse, to avoid a data breach that could compromise security and confidentiality.

However, as the amount of data available grows and technology develops, there are new ways by which data can be breached. The College needs to have in place a robust and systematic process for responding to any reported data breaches, to ensure it can act legally and responsibly, and protect personal data which it processes.

Aim

The aim of this procedure is to standardise the College's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated
- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact of the incident is understood, and action is taken to prevent further damage
- the ICO and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned

Data breaches and 'near misses'

What is a data breach?

Article 4 (12) of the General data protection Regulation ("GDPR") defines a data breach as: "a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

It is important to note that a potential data breach does not always involve technical systems or IT devices. Breaches can also involve paper-based and verbal information, for example a diary with personal details left in a coffee shop, or inappropriate disclosure of someone's information through conversation.

North East Scotland College is obliged under the GDPR to act in respect of such data breaches. This procedure sets out how the College will manage a report of a suspected data breach. The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported, and any necessary action is taken to rectify the situation.

A data breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy
- Human error - e-mailed, posted or faxed to the incorrect recipient
- Loss or theft of equipment on which data is stored
- inappropriate sharing or dissemination and/or inappropriate access controls - staff accessing information to which they are not entitled
- Hacking, malware and data corruption
- Information is obtained by deception or “blagging”
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data

What is a near miss?

A ‘near miss’ can be described as an unplanned event that did not lead to a data breach but had the potential to. It can also be described as a ‘data incident’ which requires some investigation to identify whether an actual breach has occurred: the initial investigation may change the status from incident to breach and invoke the full breach investigation procedure.

Near misses should be reported in the same way as breaches, using the procedures below. Once further information is gathered it will be determined whether an incident was a ‘near miss’ or is escalated as an actual breach.

In any situation where staff are uncertain whether an incident constitutes a full data breach or might be a ‘near miss’ it should be reported anyway using the procedures below. It is better to report something that can be acknowledged and that we can learn from than not report something that then escalates into a major issue.

Scope

This college-wide policy applies to all College information, regardless of format, and is applicable to all staff, students, visitors, contractors, partner organisations and data

processors acting on behalf of the College. It is to be read in conjunction with the College Data Policy, which is available on COLin and the College website.

Responsibilities

All staff

All staff have a responsibility for reporting suspected or actual data breaches as soon as possible. Staff are also responsible for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Managers

The Leadership Team members are responsible for ensuring that staff in their area comply with this policy and assist with investigations as required.

Data Protection Officer and College Lead (Director of Student Access and Information)

Both will be responsible for ensuring any reported breach is investigated, following these procedures. Suitable further delegation may be appropriate in some circumstances.

Information Security Lead

Responsible, along with the DPO and College Lead, for ensuring reported security breaches are investigated, following these procedures, and that appropriate remedial action is taken, where required. Suitable further delegation may be appropriate in some circumstances.

Vice Principal – Access and Partnerships

Responsible for ensuring all professional and technical support and risk analysis in relation to the management and containment of any breach.

Director of Marketing and Communications

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.

Procedure

1. Reporting a breach – internal reporting

Suspected data breaches should be reported promptly to the DPO as the primary point of contact: dataprotection@nescol.ac.uk and to the IT helpdesk: helpdesk@nescol.ac.uk . The report must contain full and accurate details of the incident including who is reporting the incident and what kind of data is involved. The incident report form should be completed as part of the reporting process (Appendix 1).

If a breach occurs or is discovered outside normal working hours it must be reported as soon as is practicable, taking into account the potential severity of the incident.

Once a data incident has been reported an initial assessment will be made to establish whether it is a breach, and the severity of the breach (see Appendix 2 – matrix for assessing severity of incident). All data breaches will be centrally logged by the DPO to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

Invigilation of assessment is carried out by a designated person where this is necessary to meet specified assessment conditions.

2. Reporting a breach – external reporting

Article 33 of the GDPR requires the College to notify the ICO only when the breach "is likely to result in a risk to the freedoms and rights of natural persons". Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made "without undue delay" and within 72 hours of becoming aware of it. If the College fails to do this, it must explain the reason for the delay.

A report to the ICO will be made by the DPO and must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of DPO, likely consequences of the breach and action taken.

3. Containment and recovery

The DPO and Info Sec Lead will identify who should lead on investigating and managing the breach.

- The DPO and Info Sec Lead will determine whether the breach is still occurring and if so, ensure appropriate steps are taken immediately to identify and implement any steps to contain the breach and minimise the effect.
- An initial assessment will be made, with relevant staff, to establish the severity of the breach.
- The DPO and Info Sec Lead will establish whether anything can be done to recover any losses and limit damage

- The DPO and Info Sec Lead will establish who may need to be notified as part of the initial containment
- The DPO and Info Sec Lead, in liaison with relevant staff, will determine a suitable course of action to ensure resolution of the incident
- The DPO and Info Sec Lead should consider whether the Director of Marketing and Communications should be informed at this stage, to prepare external or internal communications and be ready to handle enquiries.

4. Assessment of risks

- An investigation will be undertaken by the DPO or Info Sec Lead immediately and whenever possible within 24 hours of the breach being discovered/reported.
- All data security breaches will be managed according to risk. After the identification of the breach, the risks associated with the breach will be assessed in order to identify an appropriate response. Appendix 1 should be used to identify the exact nature of the breach and the severity; this information can then be used to establish the action required.
- The investigation will take into account:
  - the type of data involved and its sensitivity
  - the protections which are in place (e.g. encryption)
  - what's happened to the data, has it been lost or stolen
  - whether the data could be put to any illegal or inappropriate use
  - who the individuals are, number of individuals involved and the potential effects on those data subject(s)
  - whether there are wider consequences to the breach

5. Consideration of further notification

- The DPO and College Lead and/or Info Sec Lead and the Senior IT management team will, in consultation with the Vice Principal – Access and Partnerships, determine who needs to be notified of the breach.
- Ultimately, the DPO will decide whether the ICO should be notified of the breach within the required 72 hours
- Use of the severity matrix will help determine the risk to people's rights and freedoms and will aid the decision to notify the ICO (and the data subject(s)).
- Every incident will be assessed on a case by case basis, considering:
  - 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 DPO and/or College Lead will also consider notifying third parties such as the police, insurers and trade unions. This would be appropriate where illegal activity is known or believed to have occurred, or there is a risk of illegal activity happening in the future.

- Notification to the individual(s) whose personal data has been affected by the incident will include a factual description of how and when the breach occurred and the data involved, along with actions taken by the College. Individuals will also be provided with the name and contact details of the College DPO for further information.

- All decisions and actions will be documented by the DPO.

6. Evaluation and response

- Once the initial incident is contained, the DPO and/or Info Sec Lead will carry out a full review of the causes of the breach, the effectiveness of the response and determine whether any changes to systems, policies or procedures should be made

- 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

  - If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by College's Senior Management Team and in more serious cases it may be appropriate to report to the College Board or appropriate Committee.

Throughout the breach management process a record should be kept of actions taken and by whom. An activity log recording the timeline of the incident management will also be completed. Appendix 4 provides an activity log template to record this information. Copies of any correspondence relating to the breach should also be retained.

7. Breaches received as complaints

There are occasions when a data subject may make the college aware of a data breach by using the college's complaints procedure. If this is the case, the Head of Quality Enhancement & Transitions will forward the complaint to the Data Protection Officer to be dealt with as a data breach.

The complainant will receive acknowledgement from the College informing them that this will be handled in line with the College's Breach Reporting Procedure.
The dataprotection@nescol.ac.uk inbox will be copied into all communications with the complainant. The complaint will be sent to the DPO and this will not be counted in the complaint reporting process.

8. Disciplinary

Staff, students, contractors, visitors or partner organisations who act in breach of college policy and procedure may be subject to disciplinary procedures or other appropriate sanctions.

9. Contacts

Data Protection Officer: dataprotection@nescol.ac.uk

College Lead - Data Protection: ltaylor@nescol.ac.uk

Information Security Lead: ma.johnson@nescol.ac.uk

IT Helpdesk: helpdesk@nescol.ac.uk

Status:	Approved for Use
Date of Version:	October 2018
Responsibility for Procedure:	Director of Student Access & Information
Responsibility for Implementation:	Heads of Faculty
Responsibility for Review:	Director of Student Access & Information
Date of EIA:	October 2018
Review Date:	October 2019

.

APPENDIX A – DATA INCIDENT REPORTING FORM

Sections 1 and 2 must be completed as part of the initial report.

Please complete those sections as soon as possible and email it to the Data Protection Officer: dataprotection@nescol.ac.uk without delay. This form should also be added to the IT Helpdesk call that was initiated as part of the response.

Circulation of this form and any related documents must be restricted to those directly involved in the investigation.

Do not refer to any data subjects by name in this report.

Section 1	**Details of person reporting the incident**
Name	
Job title	
Department	
Date of report	
Section 2	**Details of the incident**
Date and time incident was discovered	
Brief description of event and circumstances – time, date, location, how it occurred, etc	
Has there been any delay in reporting this? If yes, please explain the reason(s)	Yes / No
Did the incident involve personal data? If no, submit the form now If yes, complete the rest of this section	Yes / No
Describe the type of personal data compromised. Give as much detail as possible	

Was any sensitive data compromised? (eg health info, race, ethnic origin, religious or political beliefs)	Yes / No
Described the type of sensitive personal data compromised. Give as much detail as possible	
Is the breach contained or ongoing?	Yes / No
What steps were/will be taken to contain the breach?	
When was the breach contained?	
If data is lost or stolen, what steps are being taken to recover the data? If recovered, what steps were taken?	
Section 3	**Personal data compromised**
Number of individuals whose personal data has been compromised	
Types of individual(s) whose data has been compromised – student, staff, job applicant, alumni, children, etc	
Are the affected individuals aware of the incident?	Yes / No
Have any of the individuals affected complained about the incident?	Yes / No
Section 4	**Containment and recovery**
Details of any measures in place to prevent an incident like this occurring eg encryption, back-up, training, policy	
Details of any 3rd party service providers involved in the breach	

Please provide extracts or links to any policies and/or procedures that are relevant to this incident eg information security policy	
Section 5	**Assessment of risks**
Is the information unique? Can it be restored or is it lost completely? Will its loss have an adverse effect on college business?	
Is the data bound by any contractual security arrangements? Inc. a data sharing agreement. Describe	
Section 6	**Further notification**
Have the Vice Principal – Access and Partnerships and Principal been informed?	
Does the ICO require to be informed?	
Does the data subject(s) require to be informed?	
Do the Police or other regulatory authority need to be informed?	
Section 7	**Evaluation and response**
Description of action taken in response to the incident	
Has the person(s) responsible for or involved in the incident undertaken data protection	

training? If yes please state what and when	
What steps/actions can be taken to minimise the possibility of a repeat of such an incident?	
Section 8	**Overall assessment**
Incident reference	
Incident severity (using severity matrix) Breakdown calculation of score	
Overall assessment – likely to result in: **A – no risk to the data subject** **B – risk to the data subject** **C – high risk to the data subject** Provide explanation for decision	

APPENDIX B – MATRIX FOR ASSESSING SEVERITY OF INCIDENT

Data subjects affected

Description	Scenario	Code letter	Risk rating
Very high	1000+	VH	5
High	500 – 999	H	4
Medium	100 – 499	M	3
Low	10 – 100	L	2
Very low	0 – 10	VL	1

Impact

Description	Score	Code letter	Risk rating
Very high	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).	VH	5
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).	H	4
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).	M	3
Low	Individuals may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)	L	2
Very low	No evidence that individuals will be materially affected.	VL	1

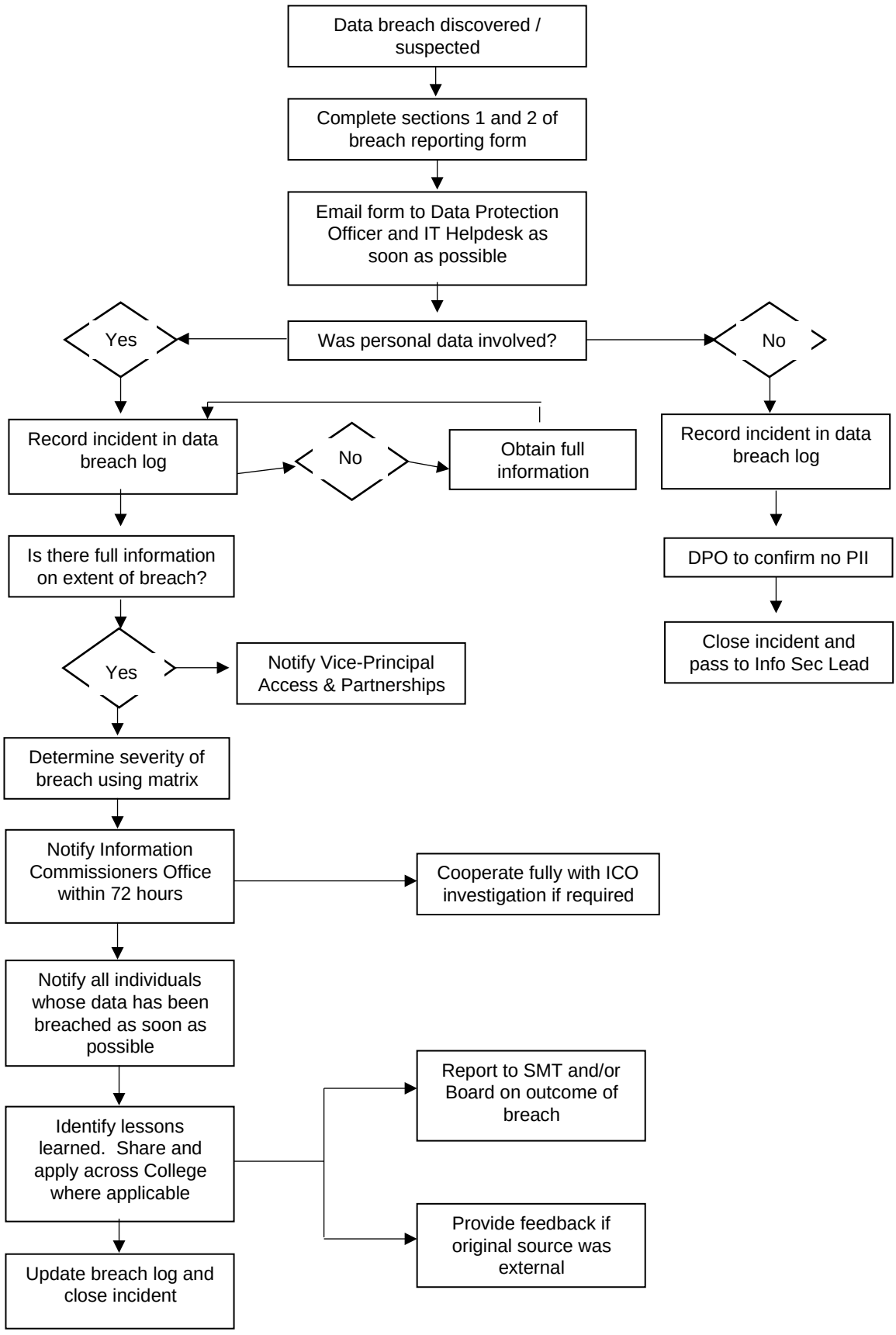
Severity

Score = Data subjects affected x impact score

Description	Score	Notify ICO	Notify data subjects
Very high	20+	Yes	Yes
High	16 – 19	Yes	Yes
Medium	11 – 15	Consider	Yes
Low	6 – 10	No	Consider
Very low	1 – 5	No	No

A final decision about notification to ICO, and whether to inform the data subjects will be made by the DPO.

APPENDIX C – DATA BREACH FLOWCHART



APPENDIX 4 – ACTIVITY LOG

Date / Time	Activity Activity, Decision, Instruction, Briefing (A,D,I,B)	Action	Owner	Completed
10/08/18 – 13.25	B – Received notification of data being encrypted on shared drive	Inform server team to close down share access on shared drive	MJ	

Completed by……

Equality Impact Assessment (EIA) Form

Part 1. Background Information. (Please enter relevant information as specified.)

Title of Policy or Procedure. Details of Relevant Practice:	Procedure 1095: Data Breach Reporting Procedure
Person(s) Responsible.	Director of Student Access & Information
Date of Assessment:	08/10/18
What are the aims of the policy, procedure or practice being considered?	Leave blank if these are already explicit on the existing paperwork.
Who will this policy, procedure or practice impact upon?	All students, staff and members of the public who have business with NESCol.

Part 2. Public Sector Equality Duty comparison (Consider the proposed action against each element of the PSED and describe potential impact, which may be positive, neutral or negative. Provide details of evidence.)

Need	Impact	Evidence
• **Eliminating unlawful discrimination, harassment and victimisation**	This procedure ensures all students are treated equally regardless of any protected characteristics that may apply. **(positive impact)**	Regulatory body guidance and codes of practice were consulted.
• **Advancing Equality of Opportunity**	The procedure ensures that the personal data is protected for all and that any breaches are dealt with in an equitable manner for all data subjects. **(positive impact)**	Inherent to data breach reporting procedure is the requirement to protect the rights and freedoms of all data subjects.
• **Promoting Good relations**	Providing a consistent and equitable process promotes good relations for all data subjects.	An identified process should provide assurance of appropriate handling to all data subjects.

	(positive impact)	

Part 3. Action & Outcome (Following initial assessment, describe any action that will be taken to address impact detected)

- The Procedure will be updated as per the review date
- The EIA may be reviewed and updated following any internal or external changes

Sign-off, authorisation and publishing *	
Name:	Linda Taylor
Position:	Head of Student Access & Information
Date of original EIA:	08/10/18
Date EIA last reviewed:	October 2018

**Please note that an electronic sign-off is sufficient*