Personal Data Breach Protocol

1. Introduction

1.1. In order to deliver our mission to provide outstanding adult residential and community education the college processes and shares a large amount of personal data about our staff, students and other individuals who interact with us.

1.2. The college takes data security very seriously and has procedures and security measures in place to guard against unlawful or unauthorised processing and against accidental loss or damage. By using appropriate technical and organisational measures every care is taken to protect data from incidents which could result in a personal data breach.

1.3. The focus of this breach response protocol is the protection of individuals and their personal data. It has been implemented to ensure that all college personnel are aware of what a data breach is and provide a framework for the containment and management of a breach in order to minimise risk, identify appropriate reporting mechanisms and identify actions to secure personal data and prevent any further breach.

1.4. This protocol applies to all personal data held by the college and to both confirmed and suspected breaches.

1.5. This document should be read in conjunction with the college's data protection policy.

1.6. All college personnel will be made aware of this protocol when they commence at the college and may be directed to periodic revisions. This protocol does not form part of any college personnel's contract of employment and the college reserves the right to change this it at any time. All college personnel are obliged to comply with this protocol at all times.

2. Definitions

College – The Northern College for Residential Adult Education Ltd.

College Personnel – Any college employee or contractor who has been authorised to access any of the college's personal data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the college.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Officer – The data protection officer is Sarah Johnson, and can be contacted at: 01226 776005, dpofficer@northern.ac.uk.

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Personal Data – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

Special Categories of Personal Data - Personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

3. **What is a Data Breach?**

3.1. A personal data breach is defined very broadly and is effectively any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of personal data. Whilst most personal data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

3.2. A personal data breach could include any of the following:

3.2.1. loss or theft of personal data or equipment that stores personal data;

3.2.2. inappropriate access controls meaning unauthorised college personnel can access personal data;

3.2.3. any other unauthorised use of or access to personal data;

3.2.4. deleting personal data in error;

3.2.5. human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing personal data on a train);

3.2.6. hacking attack;

3.2.7. infection by ransom ware or any other intrusion on our systems/network;

3.2.8. 'blagging' offences where information is obtained by deceiving the organisation who holds it;

3.2.9. destruction or damage to the integrity or accuracy of personal data.

3.3. A personal data breach could also include:

3.3.1. equipment or system failure that causes personal data to be temporarily unavailable;

3.3.2. unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;

3.3.3. inability to restore access to personal data, either on a temporary or permanent basis; or

3.3.4. loss of a decryption key where personal data has been encrypted because this means the college cannot restore access to the personal data.

3.4. This list is not exhaustive.

4. **Data Breaches by the College's Data Processors**

4.1. As well as breaches potentially occurring directly from college data sources breaches could also occur where the college uses a third party data processor.

4.2. Where the college uses a third party processor the requirements for breach reporting are detailed in the contract between the college and the processor. This includes a requirement for the processor to inform the college without undue delay if it becomes aware of a potential breach.

Data Breach Response Plan

5. **Reporting a potential data breach**

5.1. College personnel must immediately notify any confirmed or suspected personal data breach to the data protection officer, no matter how big or small and whether or not college personnel think a breach has occurred or is likely to occur. This allows the college to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the college.

5.2. If college personnel discover a personal data breach outside working hours they must notify the college's data protection officer as soon as possible.

5.3. College personnel may be notified by a third party (e.g. a supplier that processes personal data on the college's behalf) that they have had a breach that affects college personal data. Reports of potential data breaches may also be received from individual data subjects, including current and past students. Any member of staff who becomes aware of a potential breach of personal data held by the college is responsible for reporting it at the earliest possible opportunity.

5.4. A timely response is critical. The college not only has a responsibility to report any breaches to the Information Commissioner with 72 hours of becoming aware of it, it also needs to ensure that it acts without delay in order to protect those individual data subjects involved from any possible adverse consequences of the breach.

5.5. The breach/potential breach should be reported by contacting the data protection officer (DPO) – Sarah Johnson either in person, by telephone on 01226 776005 or via email to dataprotectionofficer@northern.ac.uk. Emails should have the subject line "Data Breach Report – URGENT". In the absence of the data protection officer the breach should be reported to the vice principal.

5.6. As much of the following information should be provided as possible:

5.6.1. the data affected;
5.6.2. how many individuals' records have been affected;
5.6.3. the current situation – has the breach been contained and if not, how many people could potentially have access to the affected data;
5.6.4. what action has been taken to resolve the breach;
5.6.5. how the breach happened;
5.6.6. when the breach occurred/began;
5.6.7. any other relevant details.

6. **Initial Investigation**

6.1. An initial investigation into the potential breach will be undertaken by the DPO immediately notification is received.

6.2. This initial investigation will be used to inform whether an actual breach has occurred, and if so what actions are required to contain it and what formal notification is required.

6.3. The DPO will assess the risks associated with the data involved, taking into account:

6.3.1. its sensitivity;
6.3.2. the protections in place (e.g. encryptions);
6.3.3. what has happened to the data e.g. has it been lost, corrupted, stolen;
6.3.4. whether the data could be put to any illegal or inappropriate use;
6.3.5. who the individuals affected are, the number of individuals involved;
6.3.6. the potential adverse effects on any data subjects (e.g. possibility of identity theft or other fraud/theft), how serious or substantial these are and how likely they are to occur;
6.3.7. whether there are any wider consequences to the breach.

6.4. Information from the ICO and the Article 29 Working Party guidelines on personal data breach notification will be used to inform this risk assessment process.

6.5. If it is established that the breach is unlikely to result in a risk to the rights and freedoms of the individuals affected then it will be added to the college's data breach register and no further action will be taken.

7. **Containment and Recovery**

7.1. Where it is established that a data breach has occurred which will impact on the rights and freedoms of the individuals affected then the DPO, working with other relevant college staff, will:

7.1.1. determine if the breach is still occurring. If so appropriate steps will be taken immediately to minimise the effect of the breach;

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

7.1.3. establish who may need to be notified as part of the initial containment and inform the police, where appropriate.

7.2. Input and advice from a range of staff from across the college may be required as part of this process.

8. **Notification**

8.1. Based on the outcome of the initial investigation and with due regard to data protection law and guidance provided by the Information Commissioner the DPO, in consultation with the vice principal, will determine who needs to be notified of the breach (see flow chart at appendix A).

8.2. The college may have to notify the ICO and also possibly the individuals affected about the personal data breach.

8.3. Any notification will be made by the data protection officer. The notification shall comply with the requirements of the ICO.

8.4. Notification of a personal data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the college becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals.

8.5. Notification of a personal data breach must be made to the individuals affected without undue delay where the breach is likely to result in a high risk to the rights and freedoms of individuals.

Information Commissioner	
When is notification to the ICO required?	Notification to the ICO is mandatory where there is a likely risk to people's rights and freedoms as a result of a breach which could result in physical, material or non-material damage to natural persons such as: • loss of control over their personal data; • limitation of their rights; • discrimination; • identity theft or fraud; • financial loss; • unauthorised reversal of pseudonymisation; • damage to reputation; • loss of confidentiality of personal data; • any other significant economic or social disadvantage to the natural person concerned. Breaches that are unlikely to result in a risk to the rights and freedoms of natural persons do not require notification to the ICO. An example might be where personal data is already publically available and a disclosure of such data does not constitute a likely risk to the individual. If further investigation uncovers evidence that the security incident was in fact

	contained and no breach actually occurred the ICO will be notified. There is no penalty for reporting an incident that ultimately transpires not to be a breach.
Timescale	Without undue delay, but not later than 72 hours after the college has become aware of the breach. If notification is made after 72 hours reasons for the delay must be provided. Where full details of the breach are not immediately available the college may notify the ICO in stages. Where this is the case the college will inform the ICO of its intention to provide more information later on and agree with them how and when the additional information should be provided.
How	By contacting the ICO dedicated personal data breach helpline on 0303 123 1113. Normal opening hours are Monday to Friday between 9am and 5pm.
What information should be provided?	When reporting a breach the following information will be provided: • a description of the nature of the personal data breach including, where possible; • the categories and approximate number of individuals concerned; • the categories and approximate number of personal data records concerned; • the name and contact details of the data protection officer; • a description of the likely consequences of the personal data breach; • a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.
Data Subjects	
When should individual data subjects be notified?	If a breach is likely to result in a high risk to the rights and freedoms of individuals they must be informed directly and without undue delay. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO, not all breaches will be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue. The severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring will be assessed on a case by case basis. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves, particularly if there is a need to mitigate an immediate risk of damage to them. The ICO has the power to compel the college to inform affected individuals if they consider there is a high risk. Notification to individuals is not required where: • The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it e.g. state-of-the-art encryption; • Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise e.g. taken action against the individual who has accessed personal data before they were able to do anything with it. • It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or

	are not known in the first place. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.
Timescale	Without delay. In exceptional circumstances where the risk is significantly high this might even take place before notifying the ICO.
How	By transparent and direct communication methods. Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. The college will choose a means that maximises the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean employing several methods of communication.
What information should be provided?	The college will provide: • A description of the breach in clear and plain language; • The name and contact details of the data protection officer; • A description of the likely consequences of the personal data breach; • A description of the measures taken, or proposed to be taken, to deal with the personal data breach; • Where appropriate the measures taken to mitigate any possible adverse effects; • Where appropriate specific advice on how individuals can protect themselves from possible adverse consequences of the breach, such as resetting passwords.
Chair of Audit Committee	The chair of the audit committee will be informed of any data breaches where notification to the ICO and/or data subjects is required. Where the DPO considers them to be sufficiently serious or indicative of potential systemic issues they will also be informed of any near misses or data breaches which do not require formal notification.
Other Authorities	The college may also be required to notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

9. **Breaches Not Requiring Notification**

9.1. In any cases where notification to either the ICO or individual data subjects is not required a detailed record of why this decision was made will be documented.

10. **Assessment of On-going Risks**

10.1. Once the breach has been contained the College will consider the on-going risks to the College and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach.

11. **Evaluation and Response**

11.1. Once the incident is contained and relevant notifications have been made the DPO will carry out a detailed review of the causes of the breach, the effectiveness of the response and whether any changes to systems, policies and procedures should be undertaken.

11.2. A report recommending any changes to systems, policies and procedures will be considered by the college's senior leadership team.

11.3. The DPO will ensure that any learning outcomes of the breach are shared internally as appropriate.

11.4. A report documenting details of any data breach, the actions and response taken and any lessons learnt will be submitted to the Audit Committee for consideration.

Area	Data Protection
Sub Area	Data Breach Protocol
Prepared By	Sarah Johnson, Data Protection Officer
Approved By	Senior Leadership Team
Document Manager	Sarah Johnson, Data Protection
Last Updated	May 2018
Next Review Date	May 2020

Appendix 1
Personal Data Breach Report Form

Stage 1 – Notification of Potential Personal Data Breach	
Date incident discovered.	
Date of incident.	
Name of person reporting the incident.	
Description of the incident and the personal data potentially affected.	
Description and number of data subjects affected.	
Description of any action taken at the time of discovery.	
Date information received by the data protection officer.	

Stage 2 – Initial Containment, Investigation and Assessment of Severity	
Is the breach still occurring?	yes/no
What actions are being taken to contain the breach, recover any losses and limit potential damage?	
Description of the data affected.	

Is any special category data included?	✓	Description
race		

ethnic origin		
politics		
religion		
trade union membership		
genetics		
biometrics (where used for ID purposes)		
health		
sex life		
sexual orientation		
Is any data relating to criminal offences included?		
How many data subjects are affected?		
Description of how the data is affected e.g. .		
Are any other organisations involved (e.g. third party processors)?		
Is any data that could be used to commit identity fraud included? For example: • bank details; • financial information; • national insurance number (or equivalent); • passport data; • visa data.		
Does the data include anything that could potentially cause significant damage or distress? For example: • work performance; • salary data; • disciplinary/grievance information; • sensitive negotiations.		

Stage 3 – Decision Making	
Has a data breach occurred?	Yes/No
Does the breach need reporting to the ICO?	Yes/No
Outline the basis for this decision.	

Do the individuals affected require notifying?	Yes/No
Outline the basis for this decision.	
Does anyone else need to be notified? If so who?	

Stage 3 – Containment	
Date/time breach contained.	
Description of how the breach was contained	

Stage 4 – Notifications	
ICO	date/time/description of how notified
Data subjects	date/time/description of how notified
Other	who (e.g. police) date/time/description of how notified
Risk register updated?	
Breach recorded on data breach register/data register?	

Stage 4 – Investigation
Description of investigation undertaken and outcome (attach report to senior leadership team).

Actions taken to avoid reoccurrence.