Policy Title	**Data Protection Policy**
Who does the policy apply to?	All College employees, including agency staff, contractors and those working under self-employed arrangements.
Aims	Sets out the basis on which the College will collect and process personal data.
Should be read in conjunction with	Data protection procedures and guidance Staff Code of Conduct ICT User Policy
Further advice may be sought from	The Data Protection Officer.
Review arrangements	This policy will be reviewed every three years to ensure its continuing relevance and effectiveness. The College may review the policy prior to this date should operational and/or legislative/guidance matters require it. Further details regarding revisions, the consultation and approval process and review cycle can be found at para 21 below.

1. Introduction

1.1. In order to deliver its mission to provide outstanding adult residential and community education for the empowerment and transformation of individuals and communities the College needs to collect, use and store personal data about a range of individuals including its employees, suppliers, students, governors, parents and visitors.

1.2. Protecting the confidentiality and integrity of that data is a key responsibility of everyone within the College.

1.3. The College takes data security very seriously and recognises that having controls around the collection, use, retention and destruction of personal data is essential, not only to protect the data of the individuals concerned but also in order to comply with its obligations under data protection law.

1.4. The College has implemented this data protection policy to ensure all College personnel are aware of what they must do to ensure the correct and lawful treatment of personal data.

2. Legal Framework

2.1. Northern College is the data controller as defined in the Data Protection Act 1998, EU General Data Protection Regulation (GDPR) and the Data Protection Bill 2018.

2.2. The College's Data Protection officer is Sarah Johnson who can be contacted on 01226 776005 or at dpofficer@northern.ac.uk. In the absence of the Data Protection Officer any issue needing urgent attention relating to the provisions of this policy should be raised with the Vice Principal.

2.3. The College is registered as a data controller under the Data Protection Act 1998 – registration number Z6656286. This means that the purposes for which the College collects and processes personal data are notified to and registered with the Information Commissioner's Office (ICO).

3. About This Policy

3.1. This policy (along with the other policies and documents referred to in it) sets out the basis on which the College will collect and use personal data, either where the College collects it from individuals

itself or where it is provided to the College by third parties. It also sets out rules on how the College uses, transfers and stores personal data.

3.2. It applies to all personal data stored electronically, in paper form, or otherwise.

3.3. College personnel will be provided with access to this policy when they commence working with the College and may be directed to periodic revisions. This policy does not form part of any member of the College personnel's contract of employment and the College reserves the right to change this policy at any time. All members of College personnel are obliged to comply with this policy at all times. Any failure to follow the policy may result in disciplinary action.

3.4. If you have any queries concerning this policy or how it has been followed in respect to your own personal data please contact your line manager or the Data Protection Officer.

3.5. The policy should be read in conjunction with:
3.5.1. Data Breach Protocol;
3.5.2. Privacy Notices;
3.5.3. A Guide to Your Rights – Personal Data;
3.5.4. Data Retention Policy;
3.5.5. Model Contract Terms - Data Protection;
3.5.6. Data Protection Impact Assessment Procedure;
3.5.7. CCTV Code of Practice;
3.5.8. Data Protection Staff Guidelines;
3.5.9. Data Protection Guidelines for Students.

4. Definitions

4.1. **College** – The Northern College for Residential Adult Education Ltd.

4.2. **College Personnel** – Any College employee, worker or contractor who accesses any of the College's personal data and will include employees, consultants, governors, contractors and temporary personnel hired to work on behalf of the College.

4.3. **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use personal data.

A Controller is responsible for compliance with data protection laws. Examples of personal data the College is the controller of include employee details or information the College collects relating to students. The College will be viewed as a controller of personal data if it decides what personal data the College is going to collect and how it will use it.

A common misconception is that individuals within organisations are the controllers. This is not the case it is the organisation itself which is the controller.

4.4. **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.

4.5. **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

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

4.7. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the college has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

4.8. **Personal Data** – Any information about an individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "special categories of personal data" and are defined below. Special categories of personal data are given extra protection by data protection laws.

4.9. **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses personal data on the instruction of a controller.

A processor is a third party that processes personal data on behalf of a controller. This is usually as a result of the outsourcing of a service by the controller or the provision of services by the processor which involve access to or use of personal data. Examples include where software support for a system, which contains personal data, is provided by someone outside the business; cloud arrangements and mail fulfilment services.

4.10. **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. Special categories of personal data are subject to additional controls in comparison to ordinary personal data.

5. College Personnel's General Obligations

5.1. All College personnel must:

5.1.1. comply with this policy;
5.1.2. ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties;
5.1.3. not release or disclose any personal data outside the College, or inside the College to College personnel not authorised to access it, without specific authorisation from their manager or the Data Protection Officer;
5.1.4. take all steps to ensure there is no unauthorised access to personal data;
5.1.5. ensure that personal data is stored securely at all times.

6. Data Protection Principles

6.1. When using personal data the College will comply with data protection laws by ensuring that personal data is:

6.1.1. processed lawfully, fairly and in a transparent manner;
6.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
6.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
6.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible;
6.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and
6.1.6. 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.

6.2. In addition to complying with the above requirements the College must demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this policy and the documentation referred to in it, to ensure that it can demonstrate its compliance.

7. Lawful Use of Personal Data

7.1. In order to collect and/or use personal data lawfully the College must show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

7.2. In addition when the College collects and/or uses special categories of personal data, it must show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

7.3. The College has carefully assessed how it uses personal data and how it complies with the obligations set out in paragraphs 7.1 and 7.2.

7.4. In most cases the College's legal grounds for processing personal data will be:

7.4.1. because the processing is necessary for the College to perform its contract with an individual; or
7.4.2. because the processing is necessary for the College to comply with a legal obligation; or
7.4.3. because the processing is necessary for the performance of a task carried out in the public interest.

7.5. In some circumstances the College will seek the individual's consent to process their personal data for a particular purpose.

7.6. The College sets out the legal grounds for its processing in privacy notices which are published on its website at www.northern.ac.uk/dataprotection.

7.7. If the College changes how it uses personal data it will update this record and notify individuals about the change where appropriate.

7.8. Where the College is proposing to change how personal data is used this must be notified to the Data Protection Officer who will advise whether the intended use is appropriate, update documentation as required and advise regarding any other controls required.

8. Transparent Processing – Privacy Notices

8.1. Where the College collects personal data directly from individuals it will inform them about how it will use their personal data. This will be done via a suite of privacy notices. The College has adopted the following privacy notices:

8.1.1. Privacy Notice – Students
8.1.2. Privacy Notice – College Personnel
8.1.3. Privacy Notice – Governors
8.1.4. Privacy Notice – Children
8.1.5. Privacy Notice – Additional Learning Support

8.2. Where the College receives personal data about an individual from other sources it will provide the individual with a privacy notice about how the College will use their personal data. This will be provided as soon as reasonably possible and in any event within one month.

8.3. If the College changes how it uses personal data it may need to notify individuals about the change. If College personnel therefore propose to change how they use personal data they must notify the Data Protection Officer.

9. Data Quality – Ensuring the use of accurate, up to date and relevant personal data

9.1. Data protection laws require that the College only collects and processes personal data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice and as set out in the College's record of how it uses personal data. The College is also required to ensure that the personal data the College holds is accurate and kept up to date.

9.2. All College personnel that collect and record personal data shall ensure that it is recorded accurately, is kept up to date and that collection and recording is limited to the personal data which is adequate, relevant and necessary in relation to the purpose for which it is collected and used.

9.3. All College personnel that obtain personal data from sources outside the College shall take reasonable steps to ensure that it is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College personnel to independently check the personal data obtained.

9.4. In order to maintain the quality of personal data, all College personnel that access personal data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to personal data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

9.5. The College recognises the importance of ensuring that personal data is amended, rectified, erased or its use restricted where this is appropriate under data protection laws. The College has a ***A Guide to Your Rights – Data Protection*** document which sets out how it will respond to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their personal data will be dealt with in accordance with this document.

10. Data Retention

10.1. Data protection laws require that the College does not keep personal data longer than is necessary for the purpose or purposes for which the College collected it.

10.2. The College has assessed the types of personal data that it holds and the purposes it uses it for and has set retention periods for the different types of personal data processed, the reasons for those retention periods and how the College securely deletes personal data at the end of those periods. These are set out in the College's ***Data Retention Policy***.

10.3. If College personnel feel that a particular item of personal data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College personnel have any questions about this policy or the College's personal data retention practices, they should contact the Data Protection Officer for guidance.

10.4. At the end of the retention period personal data will be disposed of securely.

11. Data Security

11.1. The College takes data security very seriously and has security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. The College has in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. These are set out in the College's ***Data Security Statement***.

12. Data Breach

12.1. Whilst the College takes information security very seriously, unfortunately it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of personal data. If this happens the College will instigate its ***Data Breach Protocol***.

12.2. Any member of College personnel who becomes aware of a potential breach of personal data held by the College is responsible for reporting it at the earliest possible opportunity in line with the College's ***Data Breach Protocol*** which can be found on the College website at www.northern.ac.uk/dataprotection.

12.3. A personal data breach 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 the actions of a member of College personnel.

12.4. There are three main types of personal data breach as follows:

12.4.1. **Confidentiality breach** – this is where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that a College personnel is not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people "blagging" access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

12.4.2. **Availability breach** – this is where there is an accidental or unauthorised loss of access to, or destruction of, personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from back up, or loss of an encryption key; and

12.4.3. **Integrity breach** – this is where there is an unauthorised or accidental alteration of personal data.

13. Appointing Contractors

13.1. Where the College appoints a contractor to process any of its personal data it will undertake sufficient data protection due diligence prior to appointment and ensure an appropriate written contract is in place.

13.2. The College will only use processors who meet the requirements of data protection law and protect the rights of individuals.

13.3. Once a processor is appointed they will be audited periodically to ensure that they are meeting the requirements of their contract in relation to data protection.

13.4. Any contract where an organisation appoints a processor will be in writing. The College has an agreed set of ***Model Contract Terms for Data Protection*** in place which will be used in most circumstances.

13.5. Every contract with a processor will contain the following obligations as a minimum:

13.5.1. to only act on the written instructions of the controller;
13.5.2. to not export personal data without the controller's instruction;
13.5.3. to ensure staff are subject to confidentiality obligations;
13.5.4. to take appropriate security measures;
13.5.5. to only engage sub-processors with the prior consent (specific or general) of the controller and under a written contract;
13.5.6. to keep the personal data secure and assist the controller to do so;
13.5.7. to assist with the notification of data breaches and data protection impact assessments;
13.5.8. to assist with subject access/individuals rights;
13.5.9. to delete/return all personal data as requested at the end of the contract;
13.5.10. to submit to audits and provide information about the processing; and
13.5.11. to tell the controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

13.6. In addition the contract will set out:

13.6.1. the subject-matter and duration of the processing;
13.6.2. the nature and purpose of the processing;
13.6.3. the type of personal data and categories of individuals; and
13.6.4. the obligations and rights of the controller.

13.7. Any member of staff proposing to appoint a data processor must contact the Data Protection Officer for advice prior to making any appointment.

14. Individuals' Rights

14.1. Data protection law gives individuals control about how their data is collected and stored and what is done with it.

14.2. The College will only use personal data in accordance with the rights given to individuals' under data protection laws, and will ensure that it allows individuals to exercise their rights. In order to facilitate this the College has a ***Guide to Your Rights – Data Protection*** document in place which outlines how individuals can exercise their rights and how the College will respond. In summary individual rights are as follows:

Subject Access Requests

14.3. Individuals have the right to ask the College to confirm what personal data they hold in relation to them and provide them with the data.

Right of Erasure (Right to be Forgotten)

14.4. Individuals have a limited right to request the erasure of personal data concerning them where:

14.4.1. the use of the personal data is no longer necessary;
14.4.2. their consent is withdrawn and there is no other legal ground for the processing;
14.4.3. the individual objects to the processing and there are no overriding legitimate grounds for the processing;
14.4.4. the personal data has been unlawfully processed; and
14.4.5. the personal data has to be erased for compliance with a legal obligation.

14.5. In a marketing context, where personal data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the personal data must not be processed for such purposes.

Right of Data Portability

14.6. An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

14.6.1. the processing is based on consent or on a contract; and
14.6.2. the processing is carried out by automated means.

14.7. This right isn't the same as subject access and is intended to give individuals a subset of their data.

The Right of Rectification and Restriction

14.8. Individuals are given the right to request that any personal data is rectified if inaccurate and to have use of their personal data restricted to particular purposes in certain circumstances.

15. Freedom of Information

15.1. Alongside data protection laws the Freedom of Information Act (FOI) 2000 gives a general right of public access to all types of recorded information held by 'public authorities'. The College falls under the definition of a public authority and is therefore covered by the act. The College has a freedom of information publication scheme which is available on the College website.

15.2. The FOI act enables individuals to ask for information about any aspect of the College's work, however this does not include personal data and requests for access to an individual's own personal information must always be handled under data protection guidelines.

16. Marketing and Consent

16.1. The College will sometimes contact individuals to send them marketing or to promote the college. Marketing consists of any advertising or marketing communication that is directed to particular individuals.

16.2. Where the College carries out any marketing it will ensure that it complies with data protection laws and only undertake marketing in a legally compliant manner.

16.3. In many cases the College may be able to market using a "soft opt in" if the following conditions were met:

16.3.1. contact details have been obtained in the course of a sale (or negotiations for a sale);
16.3.2. the College is marketing its own similar services; and
16.3.3. the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

16.4. The College will also comply with the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection.

17. The Use of CCTV

17.1. The College uses CCTV systems for the prevention and detection of crime and for protecting the security and safety of students, staff and other College users. These systems will be operated in line with the College's ***CCTV Code of Practice***.

18. Automated Decision Making and Profiling

18.1. Data protection laws provide controls around profiling and automated decision making in relation to individuals.

18.2. Automated decision making happens where the College makes a decision about an individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

18.3. Profilin**g** happens where the College automatically uses personal data to evaluate certain things about an individual.

18.4. Any proposal to introduce automated decision making or profiling must comply with data protection laws, be the subject of a data protection impact assessment.

19. Data Protection Impact Assessments (DPIA)

19.1. Where the College is launching or proposing to adopt a new process, product or service which involves personal data which is likely to result in a high risk to the rights and freedoms of individuals it will carry out a data protection impact assessment (DPIA) as part of the project initiation process.

19.2. Situations where the College may have to carry out a DPIA include:

19.2.1. large scale and systematic use of personal data for the purposes of automated decision making or profiling (see definitions above) where legal or similarly significant decisions are made;
19.2.2. large scale use of special categories of personal data, or personal data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
19.2.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.

19.3. The DPIA will be carried out at an early stage to enable the College to identify and address any potential issues relating to personal data therefore minimising risk.

19.4. In order to facilitate this process the College has in place a data protection impact assessment (DPIA) procedure.

19.5. The assessment will be completed prior to any processing commencing.

19.6. A DPIA is not a prohibition on using personal data but is an assessment of issues affecting personal data which need to be considered before a new product/service/process is rolled out. The process is designed to:

19.6.1. describe the collection and use of personal data;
19.6.2. assess its necessity and its proportionality in relation to the purposes;
19.6.3. assess the risks to the rights and freedoms of individuals; and
19.6.4. identify any measures required to address the risks.

19.7. Where a DPIA reveals risks which are not appropriately mitigated and the College wishes to proceed with the project it will consult the ICO.

19.8. All DPIAs must be reviewed by the Data Protection Officer.

20. Transferring Personal Data Outside the EEA

20.1. Data protection laws impose strict controls on personal data being transferred outside the EEA. Transfer includes sending personal data outside the EEA but also includes storage of personal data or access to it outside the EEA.

20.2. College personnel must not export any personal data outside the EEA without seeking advice from the Data Protection Officer.

21. Policy sign off and ownership details

Document Name:	Data Protection Policy
Version Number:	V2
Effective from:	31 July 2019
Next scheduled review date:	July 2022
Policy owner:	Clerk to the Governors/Data Protection Officer

22. Revision history

Version No	Effective date	Revision description/summary of changes	Author
V2	31 July 2019	Complete re-draft to reflect updated statutory requirements imposed by GDPR and Data Protection Act 2018. Largely based on AoC template.	Sarah Johnson – Data Protection Officer