

Data Protection Policy 2024-25

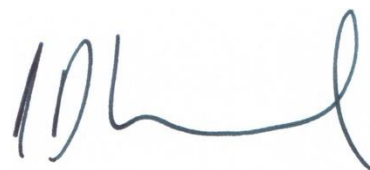
Overall responsibility:	Deputy Principal Finance & Corporate Affairs
Implementation:	Julian Wood
Date issued:	August 2024
Date for review:	July 2025

Endorsed and approved by Policy & Strategy Group

Date: September 2024

Jason Lancaster

Principal

A handwritten signature in blue ink, appearing to be "JL" followed by a stylized flourish.

1. Introduction.....	3
2. Responsibility.....	3
3. Scope.....	4
4. Policy Statement.....	4
5. Definitions.....	4
6. Key Principles.....	6
7. The Procedure.....	6
8. Reporting.....	6
9. Associated Policies.....	7
10.Approval Process.....	7
11.Appendices.....	7
Appendix 1: Lawful basis for processing personal data	
Appendix 2: Transparent processing – Privacy Notice	
Appendix 3: Data Quality	
Appendix 4: Data Retention	
Appendix 5: Data Security	
Appendix 6: Data Sharing	
Appendix 7: Data Breach	
Appendix 8: Appointing Contractors to process data	
Appendix 9: Individual’s Rights Procedure	
Appendix 10: Marketing and Consent	
Appendix 11: Data Protection Impact Assessments	
Appendix 12: Transferring Data to a country outside the UK	
Appendix 13: Help and Complaints	
Appendix 14: Equality and Diversity Impact Assessment	
Appendix 15: Data Protection Impact Assessment	
Appendix 16: Communications Plan	

1. Introduction

This policy provides a framework for ensuring that Northampton College meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

The College's reputation is dependent on the way the College manages and protects personal data. Protecting the confidentiality and integrity of personal data is a key responsibility of all employees, partners and contractors within the College. 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 management of Personal data.

All College personnel will receive mandatory induction training and have access to this policy through the Document Library. All members of College personnel are obliged to comply with this policy at all times.

This policy sets out the College's approach to the way it stores, handles and allows access to information about its employees and students; complying with the requirements of Data Protection legislation and best practice.

2. Responsibility

The Data Protection Officer is responsible for the Data Protection Policy

All College personnel must comply with this policy.

College personnel must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties.

College personnel must not release or disclose any personal data:

- outside the College; or
- within the College to College personnel not authorised to access the personal data,
- without specific authorisation from their manager or the Data Protection Officer; this includes information to be shared by phone call or email.

College Personnel must take all steps to ensure there is no unauthorised access to personal data whether by other College Personnel who are not authorised to see such personal data or by people outside the College.

3. Scope

As an organisation that collects, uses and stores personal data about its students, employees, suppliers (sole traders, partnerships or individuals within companies), student employers, governors, parents, visitors, and volunteers the College recognises that having controls around the collection, use, retention and destruction of Personal data is important in order to comply with the College's obligations under Data Protection Law.

It is expected that all members of staff adhere to these guidelines to maintain confidentiality and professionalism at all times.

4. Policy Statement

The College recognises that it has a legal duty to secure any information it holds and to only hold information which it reasonably needs to discharge its function as an employer/education provider effectively. This policy (and 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 handles uses, transfers and stores Personal data.

The College will adhere to the key principles relating to the use of data as defined in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA18).

The College will ensure that the interests of its employees and students are safeguarded by regularly reviewing the policy and by taking account of the Information Commissioner's Office Code of Practice and other advice provided by regulatory authorities.

The College will appoint a designated Data Protection Officer who will complete the annual registration for the Information Commissioner.

5. Definitions

College – Northampton College

College personnel – Any College employee, worker or contractor who accesses any of the personal data stored by the College. This includes employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

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 Law.

Data Breach – A data breach is a security incident that results in personal data the College holds being: lost, stolen, destroyed without consent, changed without consent or accessed by someone without permission. Data breaches can be deliberate or accidental.

Data Protection Law – The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and all applicable laws relating to the collection and use of personal data and privacy.

Data Protection Officer – The Data Protection Officer at Northampton College is: Julian Wood - Deputy Principal Finance & Corporate Affairs who can be contacted at: data.protection@northamptoncolleg.ac.uk

EEA – member countries of the European Economic Area: 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.

ICO – the Information Commissioner's Office, the UK's independent body set up to uphold information rights.

Individuals – Living individuals who can be identified, *directly or indirectly*, from information stored by the College. Individuals are also known as Data Subjects and include employees and non employed staff, students and former students, parents and carers, governors and trustees, local authority personnel, volunteers, visitors and applicants. Individuals also include partnerships and sole traders.

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 can include: name, address, date of birth, National Insurance Number, telephone number, email address, behaviour and attendance information, assessment and exam results, staff recruitment information, contracts and development/appraisal reviews and staff and student references. More sensitive types of data include trade union membership, genetic data

and religious beliefs. These more sensitive types of data are called “Special Categories of Personal data” and are defined in the Special Categories of Personal data below.

Processor – Processors act on behalf of, and only on the instructions of, the Controller. An entity (e.g. company, organisation or person) which accesses or uses personal data on the instruction of a Controller.

Special Categories of Personal data – some data is more sensitive and is afforded more protection. This information is related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric ID
- Health data
- Sexual life or sexual orientation
- Criminal data – including the alleged committing of an offence and the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing

In College we follow best practice guidelines from gov.uk to regard information about the following types of data as special category data:

- Safeguarding
- SEND
- Children in need
- Children looked after by a local authority

6. Key Principles

The College will adhere to the key principles relating to the use of data as defined in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA18).

The College will ensure that the interests of its employees and students are safeguarded by regularly reviewing the policy and by taking account of the Information Commissioner’s Office Code of Practice and other advice provided by regulatory authorities.

7. The Procedure

The College will appoint a designated Data Protection Officer who will complete the annual registration for the Information Commissioner.

Northampton College complies with data protection legislation guided by the six data protection principles. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- only used for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept longer than necessary; and

- kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law:

- Data Retention Guidelines
- Privacy Notice
- Subject Access Requests
- Individuals' Rights Procedure
- Data Breach Reporting

8. Reporting

Regular reporting to the Data Protection Officer, senior management and:

- Data Protection Group
- Policy & Strategy Group
- Internal / External Audit
- Recording of Data Sharing Agreements and Data Requests

9. Associated Policies

Our staff have access to a number of linked policies, operational procedures and guidance to give them appropriate direction on the application of data protection legislation, this includes but is not limited to;

-
- Administration of Medication Policy
- Artificial Intelligence Policy
- Communications Policy
- CCTV Policy
- Data Retention Guidelines
- E-Safety Policy
- Ex-offender Policy (students)
- Fitness to Study Policy
- ICT Acceptable Use Policy
- ICT Security Policy
- Individuals' Rights Procedure
- Photo Consent Policy
- Privacy Notice
- Recruitment & Selection Policy
- Recruitment of Ex-offenders Policy (staff)
- Recording of Data Sharing Agreements and Data Requests
- Safeguarding – Safer Recruitment Policy
- Safeguarding Children and Vulnerable Adults Policy

- Social Media Policy
- Staff Disciplinary Policy
- Staff Reference Guidelines
- What to do if – guides
- Working with Students Guidelines

10. Approval Process

- Policy and Strategy Group

11. Appendices

Appendix 1. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

The College has assessed the lawful bases under which it processes personal data and it complies with at least one of the lawful purposes for each type of data that it processes and stores:

- (a) Consent:** the individual has given clear consent for the college to process their personal data for a specific purpose
- (b) Contract:** the processing is necessary for a contract the college has with the individual, or because they have asked us to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (statutory regulations)
- (e) Public task:** the processing is necessary for the college to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

The college does not rely solely on student/employee consent as a legal basis, as consent can be withdrawn at any time. Withdrawing consent could mean that the college can no longer fulfil its contract to the student/employee. Consent is not available for use as a lawful basis in an employer and student employee relationship. The student employee cannot refuse to give their consent if their employer is linked to their enrolment.

There are additional conditions which are met in order to use Special Categories of personal data:

- employment and social security obligations;
- explicit consent;
- vital interests;
- necessary for establishment or defence of legal claims;
- substantial public interest; and
- various scientific and medical issues

The College has carefully assessed how it uses personal data and how it complies with the obligations placed upon it by UK GDPR and the DPA. If the College changes how it uses Personal data, the College will update this record and may also need to notify Individuals. If College personnel therefore intend to change how they use personal data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to be applied.

Appendix 2. TRANSPARENT PROCESSING – PRIVACY NOTICES

The college publishes Privacy Notices which outline how individuals' data will be used, processed and stored.

These notices contain the following information, where applicable to the use of the personal data:

- the identity and the contact details of the Controller;
- the contact details of the Data Protection Officer;
- the purposes the personal data will be used for as well as the legal basis for the processing;
- the recipients/categories of recipients of the personal data, if any;
- details of data export and the safeguards applied;
- the period the personal data will be stored;
- the right to request access to, rectification or erasure of personal data;
- the right to request restriction of use of the personal data, the right to object to use as well as the right to data portability;
- where the individual has given consent, the right to withdraw that consent;
- the right to lodge a complaint with the ICO;
- the existence of automated decision making including profiling, the logic involved, as well as the significance and envisaged consequences;
- whether the provision of the data is a statutory or contractual obligation and of the possible consequences of failure to provide such data; and
- if the Controller intends to further process the Personal data, provide the individual with information on such further processing.

The Privacy Notice is concise and provided in an easy to understand and accessible way in clear and plain language tailored for its specific audience. The Student Privacy notice is available on the college website.

Where the College collects personal data directly from individuals, the College informs them about how the College uses their personal data. For students, this information is attached as a pop-up message to each field of the online student application form, and on the Learning Agreement provided at enrolment. This information is also available in the Privacy Notice for students available on the website.

If the College receives Personal data about an Individual from other sources, the College will provide the Individual with access to a privacy notice about how the College will use their Personal data, which may relate to the privacy notice on the College website. This will be provided as soon as reasonably possible and in any event within one month.

If the College makes significant changes to how it uses Personal data, which are significantly different to what is set out in this policy and associated Privacy Notices, the College will need to notify individuals about the change. If College personnel intend to make such changes they must notify the Data Protection Officer and provide a Data Protection Impact Assessment and, where relevant, a proposed Data Sharing Agreement for review before any arrangement is entered into. The DPO and /or his / her nominee will decide whether the intended change of use requires amendments to be made to the privacy notices and any other controls and whether it can be implemented.

Appendix 3. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA FOR LIMITED AND SPECIFIED PURPOSES

Data Protection Law requires 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. The College is also required to ensure that the personal data the College holds is accurate and kept up to date.

Formal practices for the collection of up-to-date data are in place to ensure data accuracy. Checks are carried out at application and enrolment stages. If the data is inaccurate or is out of date, rectification processes are in place to make sure that it is erased or rectified.

All College personnel that collect and record personal data ensure that the personal data is recorded accurately, is kept up to date and is necessary for the purpose for which it is collected and used. All data entry staff are trained to collect the necessary data into the College's management information system.

All College Personnel that obtain personal data from sources outside the College take reasonable steps to ensure that the personal data 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.

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. 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).

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 Law. The College has an Individuals' Rights Procedure which set out how the College responds 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 should be dealt with in accordance with this document.

Training- All individuals who have access to personal data are appropriately trained in data protection. This is completed at point of employment at a New Staff Induction Day and at regular intervals via online training methods. The college's Staff Development department maintains the training record.

Appendix 4. DATA RETENTION

Data Protection Law requires that the College does not keep personal data longer than is necessary for the purpose or purposes for which the College collected it.

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 Data Retention Policy.

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 contact the Data Protection Officer for guidance.

Appendix 5. DATA SECURITY

Appropriate technical and organisational security measures are used, monitored, controlled and audited to protect against unauthorised processing, accidental loss, destruction or damage of personal data. This includes, but is not limited to:

- Multi-factor authentication
- Email quarantine
- Cyber Essentials certificate
- The use of complex passwords
- Dark web monitoring
- Sharing through encrypted documents or One Drive
- Access from abroad (for staff) only on request
- Regular in-house Phishing testing campaigns

The College takes information security very seriously and the College 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.

Appendix 6. DATA SHARING

The College can share personal data with authorised and relevant bodies and organisations in pursuance of its function, using a lawful basis under the UK GDPR, which may include law enforcement processing under Part 3 of the Act.

In addition to considering whether the data sharing achieves a benefit and is necessary, the College considers its overall compliance with data protection law when sharing data.

Step 1.

Data Protection Impact Assessment (DPIA) should be carried out as the first step where the data sharing activity or system is considered to present a high risk to the rights and freedoms of data subjects. Carrying out a DPIA is an example of best practice, ensuring openness and transparency. A DPIA helps the College to assess, and document, the risks in the planned data sharing and determine whether any safeguards need to be introduced. See *Appendix 11*.

Step 2.

Where deemed necessary, data sharing agreements set out the purpose of the data sharing, detail the type of data being shared and the lawful basis or bases for sharing. This helps all the parties involved in sharing to be clear about their roles and responsibilities. Having a data sharing agreement in place helps the College to demonstrate that it is meeting its accountability obligations under the UK GDPR.

The data sharing agreement is completed by the College staff member and the recipient organisation, forwarded to the Data Protection Officer for approval and stored in the Data Sharing Register by the Executive Office.

The UK GDPR does not prevent sharing personal data with law enforcement authorities (known under data protection law as “competent authorities”) who are discharging their statutory law enforcement functions. The UK GDPR and the DPA 2018 allow for this type of data sharing where it is necessary and proportionate.

In a situation where an individual’s life is at risk the college relies on the lawful basis of: **vital interests**. In an emergency College personnel may share data as is necessary and proportionate.

The College will develop and provide guides for staff about what to do in common circumstances, and how to assess data protection risks.

Appendix 7. DATA BREACH

A data breach is 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 access to, personal data transmitted, stored or otherwise processed.

For any data breach, the college is obliged to consider the likelihood and severity of the risk to people's rights and freedoms, and to notify the ICO unless the assessment indicates it is unlikely that there will be a risk to those rights and freedoms.

Notification must take place within 72 hours of the College becoming aware of the breach. The College's Data Protection Officer will lead on this notification process, which is shown within the What to do Guide "A data breach has occurred" below:

What to do when a data breach has occurred

Issue/background

Data breaches do occur. Breaches within educational organisations are usually the result of a lack of attention to detail and/or inadequate training. Northampton College continually raises awareness through a combination of new staff training sessions and annual online training for all staff.

Risks/Consequences

Significant damage or harm can be caused to an individual, or group of people, if information is shared to the wrong person/organisation. The Information Commissioner's Office (ICO) govern breaches and penalties.

- **Cause:** A factor that alone or in combination gives rise to risk – eg: poor security, many data subjects, personal data
- **Event:** An occurrence with some probability of happening – eg: data breach, identity theft
- **Harms:** Consequences of an event which leads to impacts - eg: anxiety, financial loss

Steps to take

Follow the Data Breach Notification steps below – the college must report the breach to the ICO within 72 hours.

1. The staff member discovers a potential data breach and reports it to the DPO via email at dataprotection@northamptoncollege.ac.uk.
2. The DPO will consider the impact of the breach and ensure the detail is recorded on the data breach register
 - If the breach is deemed to be minor with no harm to the data subject(s) the DPO will give appropriate feedback to the staff member who reported the potential breach or
 - If the breach is deemed to be serious the DPO may request additional information from the person reporting the breach and will reconsider any impact on the data subject(s)/damage/harm
3. If the damage/harm is minimal the processes in the relevant college area will be reviewed and any required training will be given or

If the damage/harm is significant the DPO may ask the reporting staff member to submit any available evidence/information

4. The DPO will report the breach as necessary to the ICO within 72 hours
 5. Any ICO instructions will be implemented
-

The College is only aware of a data breach once it has a reasonable degree of certainty that there has been a security incident and personal data has been compromised. This means that it is possible for the College to carry out a short investigation to establish whether there is a breach and the ability to do this is factored into data breach planning.

The College must also notify the individuals affected by the data breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination.

The college will not be obliged to notify the individuals affected where:

- there are technological and organisational protection measures (e.g. encryption);
- the Controller has taken action to eliminate the high risk; and
- it would involve disproportionate effort – in this case they must be informed some other way e.g. by a notice in newspapers.

The college will still have to notify the ICO where the threshold for doing so has been met.

As part of GDPR compliance the college has planned for a data breach and considered matters such as how a data breach may occur, what impact it may have and how it may be rectified.

All data breaches should be documented on an internal data breach register. In managing the risk relating to data breach there is a culture of encouraging disclosure through an internal reporting process.

If a data breach occurs college personnel comply with the college's Data Breach Notification process.

Appendix 8. APPOINTING CONTRACTORS WHO WILL ACCESS PERSONAL DATA HELD BY THE COLLEGE

If the College appoints a contractor, who is a Processor of personal data held by the College, Data Protection Law requires that the College only appoints them where the College has carried out sufficient due diligence and only where the College has an appropriate written contract in place.

The College (as Data Controller) must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, the College will consider periodic auditing where required to ensure that they are meeting the requirements of their contract in relation to Data Protection.

Any contract between the College and another organisation appointed as a Processor must be in writing.

The College would be deemed to have appointed a Processor where another organisation is engaged to perform a service for the College and as part of it they may have access to personal data held by the College. The College, as Controller, remains responsible for what happens to the personal data.

The College will ensure that, wherever practicable, any written contract with a Processor will contain the following obligations, or equivalent assurances, as a minimum, supported by an approved Data Sharing Agreement where required (see Appendix 6):

- to only act on the written instructions of the Controller
- to not export Personal data without the Controller's written instruction
- to ensure staff are subject to confidentiality obligations
- to take appropriate security measures to protect and safely store all data held
- to only engage sub-processors with the prior written consent of the Controller and under a written contract
- to assist and meet all obligations with the notification of data breaches and Data Protection Impact Assessments
- to assist and meet all obligations with subject access/individuals' rights
- to delete/return all personal data as requested at the end of the contract
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

In addition, the contract should set out:

- the subject-matter and duration of the processing
- the nature and purpose of the processing
- the legal basis for the processing

- the type of personal data and categories of individuals
- the obligations and rights of the Controller
- the obligations and rights of the Processor
- Liability clauses to protect the College against fines associated with personal data breaches caused by the Processor

Appendix 9. INDIVIDUALS' RIGHTS PROCEDURE

GDPR gives individuals control about how their data is collected and stored and what is done with it. The different types of rights of individuals are reflected in the following paragraphs.

Right of Access (Subject Access Requests)

Individuals have the right to ask the College to confirm what personal data it holds in relation to them and provide them with the data within one month and free of charge. The College can extend the time to respond by a further two months if the request is complex or if a number of requests have been received from the individual, e.g. other types of requests relating to the individuals' rights.

The individual can also ask the College to confirm:

- the purposes that the College has their data for
- the categories of personal data about them that the College has
- the recipients or categories of recipients that their data has, or will, be disclosed to
- how long the College will keep their data
- that they have the right to rectification, erasure, restriction or objection
- that they have the right to complain to the ICO if they are unhappy about how the College has dealt with their request or in general about the way the College is handling their personal data

Subject Access Requests are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

Subject Access Requests can be made on the Subject Access Request Form – supplied by the college, but the request does not need to be in writing. College personnel therefore need to be aware of what constitutes a Subject Access Request, and the process to follow.

Information requests may not be complied with if, to do so would mean disclosing information about another individual who could be identified from the requested information or if they could be put at risk. Exceptions could be made if the other individual has given explicit written consent.

If a member of the College personnel receives a request from an individual to access or to receive a copy of their Personal Data, the following procedure will be followed:

- the College personnel must forward or report the request to the Data Protection Officer as soon as they receive it (within 24 hours of receiving the request). A request from an individual does not have to be in a particular format, although best practice would be for the College to ask the individual to confirm the request in writing so it can ensure it is complying correctly with the request. If the individual does not wish to do this, then the College will confirm the request in writing and ask the individual to indicate if there are any inaccuracies. The College cannot charge a fee for responding to these requests unless a second or subsequent copy is requested (in which case the College can charge its administrative costs) or the request is unfounded or excessive.
- the Data Protection Officer will ensure that the date the request was received is recorded, and the deadline to respond and regular reminders are communicated to all College personnel involved in dealing with the request in order to track its progress;

- within 5 days of receipt, the Data Protection Officer will decide whether any further information is needed from the individual to clarify the identity of the individual or to understand the request and will ensure that the individual is asked for any further information that is needed as soon as possible.
- if further information is required, no action needs to be taken until the further information has been received from the individual.
- once the further information has been received and the College is satisfied that it knows what has been asked for, the College will begin locating the individual's personal data;
- depending on who the individual is, this may involve locating staff files, student files, information on parents, notes, minutes, correspondence and other relevant documents containing personal data either on the College's information systems, or in the College's structured paper filing systems. The Data Protection Officer will ensure College personnel know what searches they need to carry out;
- once the College has located all the personal data of the individual, the Data Protection Officer will ensure it is reviewed and decide whether any of the personal data does not need to be disclosed as there are exemptions which may apply;
- once the Data Protection Officer has decided what the College is going to provide to the individual, the College will respond providing one copy of the personal data, which, if the request is made electronically, shall be provided in a commonly used electronic form; and
- if the College fails to do this within one month of the date the College receives the request, the College will ensure that it has contacted the individual before the deadline to explain what the College has done so far and when the College aims to provide their personal data to them.

SUBJECT ACCESS REQUEST FORM

You should complete this form if you want us to supply you with a copy of any personal data we hold about you. You are entitled to receive this information under the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) 20188. We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

- ☐ Our receipt of your written request; or
- ☐ Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

SECTION 1: Details of the person requesting information

Full name:

Address:

Contact telephone number:

Email address:

SECTION 2: Are you the data subject?

(this means the person whose data you are requesting)

Please tick the appropriate box and read the instructions which follow it.

☐ **YES:** I am the data subject. I enclose proof of my identity (see below).
(please go to section 4)

☐ **NO:** I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below).
(please go to section 3)

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one or both of the following:

1) Proof of Identity

Passport, photo driving licence, national identity card, birth certificate.

2) Proof of Address

Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 3

Details of the data subject (if different from section 1)
(this means the person whose data you are requesting)

Full name:

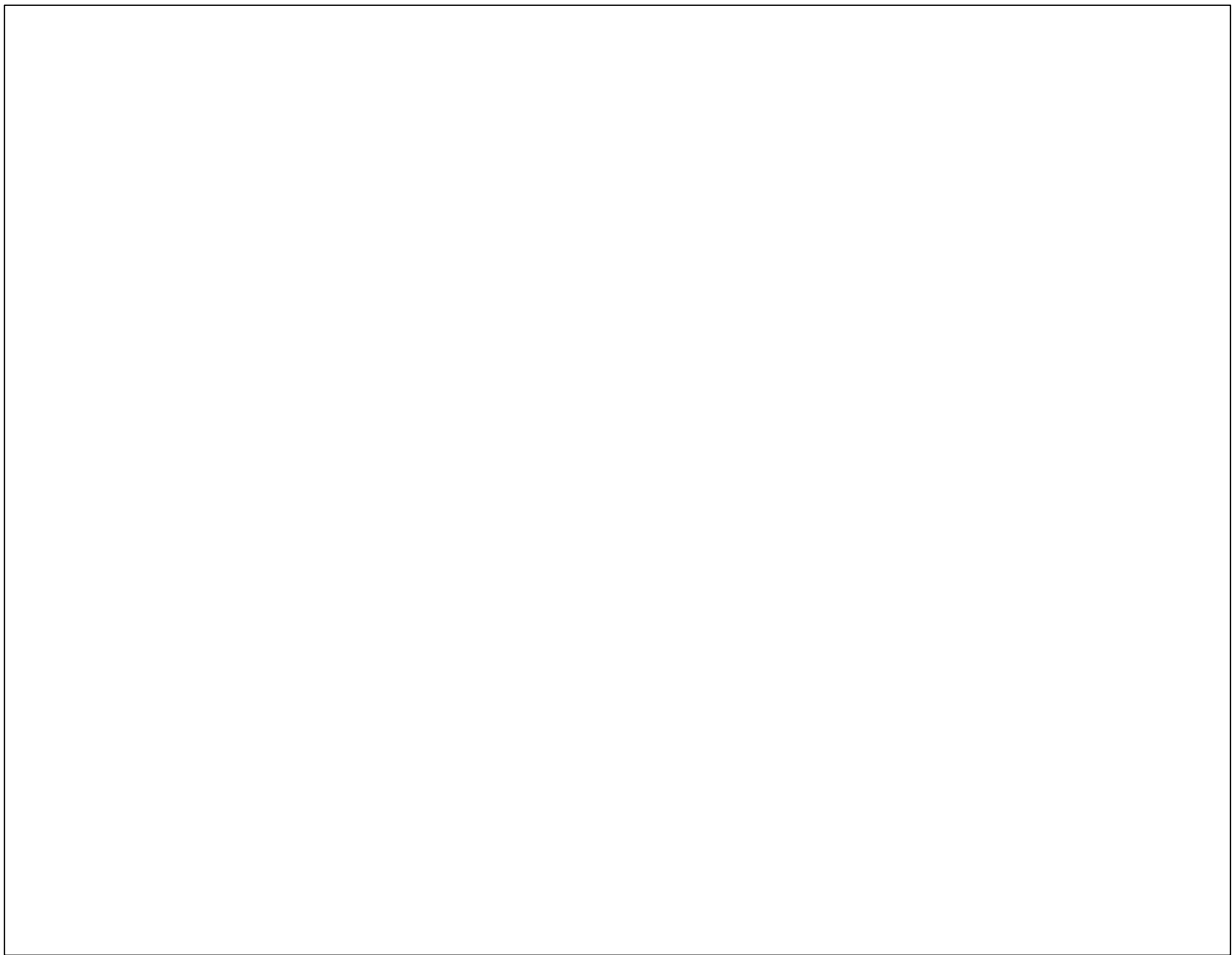
Address:

Contact telephone
number:

Email address:

SECTION 4: What information are you requesting?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.



Please note that if the information you request reveals details directly or indirectly about another individual, we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right not to provide you with copies of information requested if to do so would take “disproportionate effort”, or to charge a fee or refuse the request if it is considered to be “manifestly unfounded or excessive”. However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

SECTION 5: Information about the collection and processing of data

If you want information about any of the following, please tick the boxes:

- Why we are processing your personal data ☐
- To whom your personal data are disclosed ☐
- The source of your personal data ☐

SECTION 6: Disclosure of CCTV images

If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?

YES

☐

NO

☐

SECTION 7: Declaration

Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this Subject Access Request Form and certify that the information provided to Northampton College is true. I understand that it is necessary for Northampton College to confirm my/the data subject's identity and it may be necessary that I provide more detailed information in order for Northampton College to locate the correct personal data.

Signed..... **Date**

Documents which must accompany this application:

- ☐ **Evidence of your identity (see section 2)**
- ☐ **Evidence of the data subject's identity (if different from above)**
- ☐ **Authorisation from the data subject to act on their behalf (if applicable)**

Please return the completed form to:

Data Protection Officer
Northampton College
Booth Lane
Northampton
NN3 3RF

Email: dataprotection@northamptoncollege.ac.uk

Correcting Information

If after you have received the information, you have requested, you believe that:

- ☐ the information is inaccurate or out of date; or
- ☐ we should no longer be holding that information; or
- ☐ we are using your information for a purpose of which you were unaware;
- ☐ we may have passed inaccurate information about you to someone else;

then you should notify our Data Protection Officer at once:

Email: dataprotection@northamptoncollege.ac.uk

Help and Complaints

Northampton College takes its UK GDPR and DPA responsibilities very seriously.

Individuals who require any assistance for matters covered by DPA or GDPR should give the College the chance to rectify and resolve any issues by contacting the Data Protection Officer at dataprotection@northamptoncollege.ac.uk

If the College is unable to resolve the request, to the satisfaction of the individual, they may wish to contact the Information Commissioner's Office by live chat on ico.org.uk or the telephone helpline on 0303 123 1113.

Right to Erasure

This is a limited right for individuals to request the erasure of personal data concerning them where:

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

If the College has disclosed the individual's deleted personal data to any third parties, the College will tell the individual who those third parties are and inform the third parties to delete the personal data.

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.

If a member of the College personnel receives a request from an individual to delete their personal data, the following procedure will be followed:

- the College Personnel must forward the request to the Data Protection Officer as soon as they receive it;
- the Data Protection Officer will the date the request was received is recorded, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances) and regular reminders are sent to all College Personnel involved in dealing with the request in order to track its progress;
- the Data Protection Officer will reach a decision as to whether the right to be forgotten applies;
- if the right to be forgotten does apply, the Data Protection Officer will decide whether the College is required to keep any parts of the personal data for evidence reasons and, if so, this personal data will be excluded from the request;
- the College will then securely delete all the personal data about that individual that the College has which is not excluded. This will include securely shredding all hard copy documents and ensuring that computer records are securely deleted from the College's information systems in line with the processes detailed in the College's Data Retention Policy;
- the College will ascertain whether it has disclosed the deleted Personal Data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to delete the Personal Data; and
- the College will confirm to the individual in writing within one month of the date of their request that the College has complied with the request.

Right of Data Portability

Individuals have the right to obtain from the College a copy of their own personal data in a structured, commonly-used and machine-readable format (such as CSV files). The aim of this right is to facilitate the ability of individuals to move, copy or transmit their Personal Data easily from one IT environment to another.

The right to data portability only applies when:

- the individual provided the College with the personal data;
- the processing the College is carrying out is based on the individual's consent or is necessary for the performance of a contract; and
- the processing is carried out by automated means.

This means that the right to data portability does not apply to personal data the College is processing on another legal basis, such as its legitimate interests.

The College is obliged to provide this information free of charge within one month of the individual making the request (or two months where the request is complex provided that the College explains to the individual why it needs more time).

The individual also has the right to ask the College to transmit the personal data directly to another organisation if this is technically possible.

If a member of the College personnel receives a request from an individual to provide a copy of their Personal Data in a structured, commonly-used and machine-readable format, the following procedure will be followed:

- the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;
- the Data Protection Officer will ensure the date the request was received is recorded, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances), and regular reminders are provided to all College Personnel involved in dealing with the request in order to track its progress;
- the Data Protection Officer will reach a decision as to whether the right to data portability applies and to which subset of the individual's personal data it applies; and
- if the right to data portability does apply, the College will action the request as soon as possible. This will include creating an electronic copy of the individual's personal data which can be transferred to another organisation if the individual asks the College to.

The Right of Rectification

Individuals have the right to ask the College to correct any personal data about them that the College is holding that is incorrect. The College is then obliged to correct that personal data within one month (or two months if the request is complex).

Where the individual tells the College their personal data is incomplete, the College is obliged to complete it if the individual asks the College to do so. This may mean adding a supplementary statement to their personal file for example.

If the College has disclosed the individual's inaccurate personal data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties of the correction where the College can.

When an individual asks the College to correct their personal data, the College is required to do so and to confirm this in writing to the individual within one month of them making the request.

If a member of the College personnel receives a request from an individual to correct their personal data, the following procedure will be followed:

- the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;
- the Data Protection Officer will ensure the date the request was received is recorded, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances), and regular reminders, are provided to all College personnel involved in dealing with the request in order to track its progress;
- the College will then locate the personal data concerned and verify whether it is incorrect or incomplete and will correct it or complete it as soon as possible;
- the College will ascertain whether the College has disclosed the incorrect personal data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to correct the personal data;
- the Data Protection Officer will decide whether the College needs to keep a copy of the original personal data for evidence reasons or otherwise; and
- the College will confirm to the individual in writing within one month of the date of their request that the College has complied with the request.

Right to Restrict Processing

Individuals have the right to “block” or “suppress” the College’s processing of their personal data when:

- they contest the accuracy of the personal data, for a period enabling the College to verify the accuracy of the personal data;
- the processing is unlawful and the individual opposes the deletion of the personal data and requests restriction instead;
- the College no longer needs the personal data for the purposes the College collected it for, but the College is required by the individual to keep the personal data for the establishment, exercise or defence of legal claims;
- the individual has objected to the College's legitimate interests, for a period enabling the College to verify whether its legitimate interests override their interests.
- If the College has disclosed the individual's restricted personal data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties about the restriction where the College can.
- When an individual asks the College to restrict its processing of their personal data, the College is required to do so and to confirm to the individual in writing within one month of them making the request that this has been done.

If a member of the College personnel receives a request from an individual to restrict the College's use of their personal data, the following procedure will be followed:

- the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;
- the Data Protection Officer will ensure the date the request was received is recorded, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances), and regular reminders, are provided to all College Personnel involved in dealing with the request in order to track its progress.
- the Data Protection Officer will reach a decision as to whether the right to restrict processing applies.
- if the right to restrict processing does apply, the College will action the request as soon as possible and ensure that the College no longer uses the individual's personal data in the way they have objected to. This may include moving documents to folders where they can no longer be accessed, removing details from files and locking paper files away;
- the College will ascertain whether the College has disclosed the personal data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to stop using the personal data in the restricted way; and
- the College will confirm to the individual in writing within one month of the date of their request that the College has complied with the request.

The Right to be Informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

- the College provides individuals with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with
- the College provides privacy information to individuals at the time we collect their personal data from them.
- If the College obtains personal data from other sources, we provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month unless the individual already has the information or it would involve a disproportionate effort to provide it to them.
- The information the College provides to people is concise, transparent, intelligible, easily accessible, and it uses clear and plain language.
- The College regularly reviews, and where necessary, updates privacy information.

The Right to Object

Individuals have the right to object to the College's processing of their personal data where:

- the College's processing is based on its legitimate interests or the performance of a task in the public interest and the individual has grounds relating to his or her particular situation on which to object;
- the College is carrying out direct marketing to the individual; and/or
- the College's processing is for the purpose of scientific/historical research and statistics and the individual has grounds relating to his or her particular situation on which to object.

If an individual has grounds to object to the College's legitimate interests, the College must stop processing their personal data unless the College has compelling legitimate grounds for the processing which override the interests of the individual, or where the processing is for the establishment, exercise or defence of legal claims.

If an individual objects to direct marketing, the College must stop processing their personal data for these purposes as soon as the College receives the request. The College cannot refuse their request for any reason and cannot charge them for complying with it.

Before the end of one month from the date the College gets the request, the College must notify the individual in writing that the College has complied or intends to comply with their objections or that the College is not complying and the reasons why.

If a member of the College personnel receives an objection from an individual to the College's processing of their personal data, the following procedure will be followed:

- the College personnel must forward or report the request to the Data Protection Officer as soon as they receive it;
- the Data Protection Officer will ensure the date the request was received is recorded, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances), and to all College personnel involved in dealing with the request in order to track its progress;
- the Data Protection Officer will reach a decision as to whether the right to object applies;

- if the right to object does apply, the College will action the request as soon as possible. This may include suppressing the individual from the College's direct marketing lists, or stopping the processing of personal data that has been objected to; and
- the College will write to the individual within one month of the date of their request to tell them either that the College has complied with, or intends to comply with, their request or that the College has not complied and the reasons why the College has not complied.

Rights related to Automated Decision Making including Profiling

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

Profiling happens where the College automatically uses Personal data to evaluate certain things about an Individual.

Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Law. If College personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

College personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

The College does not carry out Automated Decision Making or Profiling in relation to its employees.

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is:

- necessary for entering into or performing a contract between the College and the individual;
- required or authorised by Data Protection Laws; or
- based on the individual's explicit consent.

If a member of the College Personnel receives an objection from an individual to an automated decision that the College has made about the individual which produces legal effects concerning them or similarly significantly affects them, the following procedure will be followed:

- the College personnel must forward or report the request to the Data Protection Officer as soon as they receive it;
- the Data Protection Officer will ensure the date the request was received is recorded, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances), and regular reminders, are provided to all College personnel involved in dealing with the request in order to track its progress.
- the Data Protection Officer will reach a decision as to whether the right to intervene in the automated decision-making applies.

- if the right to intervene does apply, the College will action the request as soon as possible. This will involve reviewing the automated decision-making process, reviewing the decision that was made, having College personnel consider whether the decision needs to be retaken and allowing the individual to give their view on the decision; and
- the College will write to the individual within one month of the date of their request to tell them what the outcome of the College's review is.

Requests the College does not have to respond to

If the request the College receives from an individual is unfounded or excessive then the College may either:

- refuse to action the request; or
- charge a reasonable fee taking into consideration the College's administrative costs of providing the information or taking the action requested.

Any decisions in relation to not actioning the request or charging a fee shall be made by the Data Protection Officer.

Response Times

All requests set out above will be responded to within a month unless the request is complex in which case the period may be extended up to a further two months. Any decision in relation to whether the request is complex is to be made by the Data Protection Officer who shall ensure the individual making the request is informed of the extension. Any notification of the extension to the individual shall be made within the initial one month period and shall give reasons for the delay.

If the College is not going to action the request made by an individual, the Data Protection Officer shall ensure this is communicated to them within one month of receipt of the request. The communication shall include details of the College's reasons for not actioning the request and the ability of the individual to make a complaint to the ICO.

Legal Advice

Specialist external legal advice may be taken on the above, but this shall be the decision of the Data Protection Officer.

Appendix 10. MARKETING AND CONSENT

The College will sometimes contact individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Law requires that this is only done in a legally compliant manner.

The College provides details in the Privacy Notice on the website and on the student's Learning Agreement

The College's Marketing & Communications Policy covers the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection.

The College gives individuals the opportunity to opt out of marketing communications:

- at Application stage via the online application form completed by the applicant
- at Enrolment stage - electronically, for full time students, and verbally for part time students, at Enrolment

Students' decisions of opting in or out of receiving information about Courses/Learning Opportunities and separately Surveys/Research, along with methods of contact (telephone, email, post) are recorded on the student record.

Appendix 11. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

Where the College is launching or proposing to adopt a new process, product or service which involves Personal data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process.

The College needs to carry out a DPIA at an early stage in the process so that the College can identify and overcome problems with its proposed new process, product or service, thereby reducing the associated costs and damage to reputation, which might otherwise occur.

The College must do a DPIA for processing that is **likely to result in a high risk** to individuals. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

The process is designed to:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks

To assess the level of risk, the College must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

College personnel should consult the Data Protection Officer and, where appropriate, individuals and relevant experts.

If the College identifies a high risk that cannot be mitigated, the ICO must be consulted before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, they may issue a formal warning not to process the data or ban the processing altogether.

Situations where the College may have to carry out a Data Protection Impact Assessment include, but are not limited to, the following:

- large scale and systematic use of Personal data for the purposes of Automated Decision Making or Profiling where legal or similarly significant decisions are made
- entering in to working contracts with other organisations where data processing will occur (this is in addition to ensuring that a Data Sharing Agreement is in place)
- 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
- systematic monitoring of public areas on a large scale e.g. CCTV cameras

All DPIAs must be reviewed and approved by the Data Protection Officer.

A template DPIA follows:

Data Protection Impact Assessment

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely **high risk** are involved?

Describe the scope of the processing: what is the nature of the data, and does it include **special category** or **criminal offence** data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for the college, for the students and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep?* How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

*Function creep **occurs when information is used for a purpose that is not the original specified purpose.**

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by: (Originator & Senior Dept Manager)		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by: (Data Protection Officer)		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 12. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

The UK GDPR primarily applies to Controllers and Processors located in the United Kingdom, with some exceptions. People risk losing the protection of the UK data protection laws if their personal data is transferred outside the UK.

Data Protection Law imposes strict controls on personal data being transferred outside the UK. Transfer includes sending personal data outside the EEA but also includes storage of personal data or access to it outside the UK.

Whenever the College appoints a supplier who is based outside the UK or the College appoints a supplier with group companies outside the UK (which may give access to the personal data to staff outside the UK) – the Data Protection Officer should be consulted.

So that the College can ensure it is compliant with Data Protection Law, College personnel must not export personal data to a country outside the UK unless it has been approved by the Data Protection Officer.

Appendix 13. Help and Complaints

Northampton College takes its UK GDPR and DPA responsibilities very seriously.

Individuals who require any assistance for matters covered by this policy should give the College the chance to rectify and resolve any issues by contacting the Data Protection Officer at dataprotection@northamptoncollege.ac.uk

If the College is unable to resolve the request, to the satisfaction of the individual, they may wish to contact the Information Commissioner's Office by live chat on ico.org.uk or the telephone helpline on 0303 123 1113.

Appendix 14: EQUALITY & DIVERSITY IMPACT ASSESSMENT

This template has been designed to help you take action to improve services and practices which affect staff, students and other service users at Northampton College. By completing this template, you would have considered the impact that your policy, practice or service might have on particular social groups within the college community. The exercise will also provide you with the opportunity to demonstrate, where possible, that the College promotes equity, diversity and inclusion.

Once this Equality Impact Assessment has been created, please include on the last page of your policy document.

Policy Details	
What is the policy?	Data Protection Policy
Is it new or existing?	Existing
Department	Finance
Policy Author (postholder title, name)	J Wood Deputy Principal Finance & Corporate Affairs
Author of Equality Analysis	J Wood
Date of completion	16/09/24

Aim and Objectives
Briefly describe the aims and objectives of the policy
The objective of the policy is to ensure personal data is protected and the College complies with Data Protection regulations.

Policy Assessment				
Consider whether your policy might have an impact on various groups identified within the categories listed below and explain why you have reached this conclusion.				
Please tick (✓) the identified level of impact (positive, negative, or no impact) and provide details of your findings.				
	Positive Impact	Negative Impact	No Impact	Findings

Race			✓	
Religion and/or belief			✓	
Sex (Gender)			✓	
Gender Identity			✓	
Disability			✓	
Age			✓	
Sexual orientation			✓	
Marriage and/or civil partnership			✓	
Pregnancy and/or maternity (including surrogacy and adoption)			✓	
Other identified group (e.g. carers)				

Action Planning

How do you intend to mitigate or eliminate any negative impact identified?	If a positive impact is identified, how do you intend to promote or develop this opportunity?	Where negative impact has been identified, can it be justified? If so, explain how.

Monitor and Review

How will you monitor the impact of your policy once it has been put into effect?

The policy will be monitored through feedback from services users gathered via:

- GDPR Group
- Policy and Strategy Group.
- Safety, Health, and Environment Committee.

Names and position of Impact Assessment Team (min of 3 preferably from areas across the College):

Name	
Carol Meadows	Director of MIS
Julian Wood	Deputy Principal Finance & Corporate Affairs
Alex Summers	Enrolment Centre Manager
Equality Analysis Sign-Off Signature and Date:	16.09.24
Review Date:	31.07.25

Appendix 15: DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment
Does this Policy

- require the collection and use of data in addition to that normally collected by the College?

Yes / No (if Yes complete Assessment point number 1)

- require the sharing of data with partners?

Yes / No (if Yes complete Assessment point number 2)

1. Is additional data being collected? If so, please detail:

No.

Is data collected personal and/or sensitive?

n/a

How will you collect, use, store and delete data?

n/a

2. Will you be sharing data with anyone? Please detail what data, with who and confirm a **Data Sharing Agreement** is in place

n/a

Describe the purposes of the processing / sharing: What are the benefits of the processing/ sharing – for you, and more broadly?

n/a

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

n/a

Describe compliance and proportionality measures, in particular:
What is your lawful basis for processing?

n/a

--

How will you ensure data quality and data minimisation?

n/a

What information will you give individuals?

n/a

Please attach a Risk Assessment if there are significant risks to data protection

Signed by Data Protection Officer

Name: Julian Wood

Position: Deputy Principal Finance & Corporate Affairs

Date: 16.09.24

Appendix 16: COMMUNICATIONS PLAN

TITLE OF COLLEGE POLICY:	DATE APPROVED BY
	Date: 05.05.23

AUDIENCE (select appropriate with ✓)					
Managers		Curriculum teams		Business Support teams	
All staff	Y	Suppliers		Partners	Y
Other - Students	Y				

CHANNEL (select appropriate with ✓)					
Policy & Strategy Team (PST)	Y	Quality Improvement Network (QIN)		Marketing team	
Meeting	Y	Meeting		NC Update Intranet Website	
Individual team		Suppliers		Partners	
Document Library Noticeboards Team meeting Email	Y	e.g. Letter or email Meeting		e.g. Letter or email Meeting	
College Management Team (CMT)		JCNC		CORPORATION	
Meeting		e.g. Meeting Email		e.g. Meeting Email	

COMMUNICATIONS PLAN ACTIVATED BY:		
Name: Julian Wood Department Finance & Corporate Affairs	Job title: Deputy Principal - Finance & Corporate Affairs	Date: 16.09.24