Data Protection Policy 2026-2027

Overall responsibility:	Chief Executive, on behalf of the Corporation
Implementation:	Interim Data Protection Officer, reporting to the Chief Executive
Date issued:	September 2026
Date for review:	July 2027, and on any material change to the law, to the College's processing, or on the merger taking legal effect on 1 January 2027

Submitted for endorsement and approval by Digital, Data and Systems Group

Date: September 2026

Jason Lancaster

Chief Executive



Contents

1. 1noduction....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: Record of Processing Activities
Appendix 15: Appropriate Policy Document

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 advises on and monitors compliance with this Policy under Article 39 UK GDPR. Ownership of the Policy, and accountability for decisions taken under it, rests with the Chief Executive on behalf of the Corporation. Where a decision departs from the Data Protection Officer's advice, the reasons are recorded.

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 person appointed by the College under Article 37 UK GDPR, contactable at dataprotection@northamptoncollege.ac.uk. The Data Protection Officer reports to the highest management level, must not receive instructions on how to carry out the role, and must not hold any other position within the College that determines the purposes and means of processing personal data. Any conflict of interest is recorded and managed. The current postholder is named in the Information Rights Handling Procedure.

EEA – the European Economic Area. Since the United Kingdom left the European Union the test for restricted transfers is whether the destination is covered by UK adequacy regulations, not whether it is in the EEA. The member countries of the EEA are: 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 offence data – defined separately below. It is not special category data and is governed by Article 10 UK GDPR

Criminal Offence Data – personal data relating to criminal convictions and offences, or to related security measures, within the meaning of Article 10 UK GDPR. This includes allegations, cautions, convictions, DBS outcomes and safeguarding allegations. Criminal Offence Data is not special category data and is governed by a separate regime: it requires either official authority or a condition in Schedule 1 to the Data Protection Act 2018, and in most cases an Appropriate Policy Document. Records containing the following, while not themselves special categories under Article 9, commonly contain special category or criminal offence data and are handled by the College with the same level of protection:

- 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 Article 5(1), together with the accountability principle in Article 5(2). In summary, the six principles 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:

The College maintains a record of processing activities under Article 30 UK GDPR. The record identifies, for each processing activity, the purposes, the categories of individuals and personal data, the recipients, any transfers outside the United Kingdom, the retention periods and the security measures applied. It is reviewed at least annually and is the reference point for privacy notices, retention decisions and responses to individual rights requests.

- Data Retention Guidelines
- Privacy Notice
- Subject Access Requests
- Individuals' Rights Procedure
- Data Breach Reporting
- Information Rights Handling Procedure, covering subject access requests, freedom of information requests and personal data breaches. As a further education corporation the College is a public authority for the purposes of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004, and requests under those regimes are handled through the same intake route. Each of these starts a statutory time limit from the moment it reaches anyone at the College, and must be forwarded to the Data Protection Officer the same day.

8. Reporting

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

- Data Protection Group
- Digital, Data and Systems 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

- Digital, Data and Systems 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)

(d) Vital interests: the processing is necessary to protect someone's life. The College relies on this basis in an emergency, and in the circumstances described at Appendix 6. (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. As a further education corporation the College is a public authority and relies principally on public task and legal obligation.

(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 final paragraph of Article 6(1) disapplies this basis for public authorities in the performance of their tasks. The College therefore does not rely on legitimate interests for processing carried out in the performance of its public functions. Where it is relied on for activity outside those functions, a legitimate interests assessment is recorded.

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.

Where the College relies on a condition in Schedule 1 to the Data Protection Act 2018 for special category or criminal offence data, it maintains an Appropriate Policy Document as required by Part 4 of that Schedule. The Appropriate Policy Document explains how the College complies with the principles and how long the data concerned is retained. It is kept under review and is provided to the Information Commissioner on request.

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

The College keeps personal data only for as long as it is needed for the purpose for which it was obtained, and for any period required by law, by a funding condition or to defend a legal claim.
Retention periods for every category of record are set out in the College's Data Retention Guidelines, which are maintained separately and approved alongside this Policy. A reference in those guidelines to a year means the period from 1 September to 31 August, and a period expressed in years after a course ends runs from the end of the academic year in which the course ended.
When a retention period expires, records are securely destroyed and a record of disposal is kept.
See: Data Retention Guidelines.

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 and Students) 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 GPDR, 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 personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Any member of staff who becomes aware of an actual or suspected breach must report it the same day to dataprotection@northamptoncollege.ac.uk with "DATA BREACH" in the subject line. Staff are not expected to assess how serious it is before reporting. Nothing connected with the incident may be deleted, edited or tidied: section 173 of the Data Protection Act 2018 makes it a criminal offence to alter or destroy records with the intention of preventing disclosure.

The Data Protection Officer assesses every breach and determines whether it must be notified to the Information Commissioner. Notification must be made within 72 hours of the College becoming aware. That period runs from the point at which the College becomes aware, not the point at which the Data Protection Officer is told, and it is a period of calendar hours which does not pause for evenings, weekends, bank holidays or leave. A late notification must still be made, with the reasons for the delay.

Where a processor acting on the College's behalf suffers a breach affecting College data, the obligation to notify remains with the College as controller.

Every breach is recorded whether or not it is notifiable, together with the assessment and the reasoning.

The full procedure, including the acknowledgement and escalation route and what happens during any absence of the Data Protection Officer, is set out separately.

See: Information Rights Handling Procedure, Stage 5C; and the one-page staff route "Something has gone wrong with personal data".

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 and indemnity provisions addressing loss caused by the Processor. Whether a regulatory penalty imposed on the College can lawfully be recovered from a Processor is not settled, and such clauses should not be relied on as the College's principal protection

Appendix 9. INDIVIDUALS' RIGHTS PROCEDURE

Individuals have the rights set out in Articles 12 to 22 UK GDPR: to be informed, of access, to rectification, to erasure, to restriction, to data portability, to object, and rights in relation to automated decision-making. They also have a statutory right under section 164A of the Data Protection Act 2018 to complain to the College about how it has used their personal data.

A request may be made in any form, to anyone at the College, and need not cite the law or use any particular words. No form is required. Any member of staff who receives one must forward it to dataprotection@northamptoncollege.ac.uk the same day, stating when and by what route it first arrived, and must not attempt to answer it themselves.

The time limit for responding runs from the date the request first reached anyone at the College, not from the date it reached the Data Protection Officer. For subject access it is one month, which pauses while identity is verified or the scope clarified, and may be extended by up to two months where the request is complex if the requester is told within the first month.

The procedure for handling each type of request, and the operational detail of running a subject access search, are set out separately and are maintained as free-standing documents so that they can be revised without amending this Policy.

See: Information Rights Handling Procedure, Stage 5A; and Annex A — Subject access request: operational procedure.

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.

Marketing by electronic mail and text message is governed by regulation 22 of the Privacy and Electronic Communications Regulations 2003, which applies in addition to the UK GDPR and requires either consent or a soft opt-in. Satisfying Article 6 does not by itself permit a marketing email. Consent must be a positive, recorded action, specific to the channel, and freely given. An opt-out described in a privacy notice is not consent. The College obtains and records marketing preferences separately for email, post, and telephone or text:

- 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.

The College records what was asked, the wording shown at the time, the answer given and the date, so that consent can be demonstrated. A refusal is recorded positively rather than left blank. Before any marketing is sent, records are screened against the suppression list; the right to object to direct marketing is absolute and applies in every channel. Requests to use learner or former learner data for marketing are referred to the Data Protection Officer before the data is extracted.

Appendix 11. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

A data protection impact assessment is required before processing begins wherever that processing is likely to result in a high risk to individuals. Screening is completed for every new system, supplier, process or significant change, and the screening itself is recorded whether or not a full assessment follows.

An assessment is always required in the three cases set out in Article 35(3) UK GDPR, and in the further cases listed by the Information Commissioner under Article 35(4). Where a high risk cannot be reduced, the Information Commissioner must be consulted before the processing begins, and will respond within eight weeks or fourteen weeks in a complex case.

Screening and assessment are carried out on the College's current pro forma, which is maintained separately so that it can be updated as the law and the Commissioner's guidance change, without amending this Policy.

See: Data Protection Impact Assessment pro forma; and the one-page screening route "Do I need a 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 United Kingdom, and also includes storage of personal data outside the United Kingdom and remote access to it from outside the United Kingdom. A transfer may only be made where the receiving country is covered by UK adequacy regulations, or under the International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses supported by a documented transfer risk assessment, or under another lawful transfer mechanism.

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. RECORD OF PROCESSING ACTIVITIES

The College maintains a record of its processing activities under Article 30 UK GDPR. The record identifies, for each activity, the purposes, the categories of individuals and of personal data, the recipients, any transfer outside the United Kingdom, the retention period and the security measures applied. It also records the lawful basis and, where relevant, the Article 9 or Article 10 condition. The record is maintained by the Data Protection Officer with the information asset owners, reviewed at least annually, and is the reference point for privacy notices, retention decisions, impact assessments and responses to individual rights requests.
See: Record of Processing Activities.

Appendix 15. APPROPRIATE POLICY DOCUMENT

Where the College relies on a condition in Schedule 1 to the Data Protection Act 2018 for special category or criminal offence data, Part 4 of that Schedule requires an appropriate policy document to be in place at the time of the processing.
The College maintains such a document. It explains the procedures for securing compliance with the data protection principles and the policies for retention and erasure of the data concerned, is kept under review, is retained for six months after the processing ends, and is provided to the Information Commissioner on request without charge.
See: Appropriate Policy Document.