

POLICY

Document Title	General Data Protection Policy
Version	Version 3.1
Equality Impact Assessment Status	Complete
Approved by	Board of the Corporation
Date approved	15 October 2024
Effective date	16 October 2024
Date of next review	31st July 2026
Lead responsibility	Director of Information Services

1. Overview

- 1.1. The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.
- 1.2. As an organisation that collects, uses, and stores Personal Data about its employees, suppliers (sole traders, partnerships, or individuals within companies), learners, governors, parents/guardians, employers (sole traders, partnerships, or individuals within companies), partners and visitors, 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 Laws and in particular its obligations under Article 5 of GDPR.
- 1.3. The College has implemented this Data Protection Policy to ensure all College employees are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for successful working and learning environments for all.
- 1.4. College employees will receive a copy of this Policy when they commence employment with the College and will receive periodic revisions of this Policy, as appropriate. All employees of the College are obliged to comply with this Policy.
- 1.5. If you have any queries concerning this Policy, please contact our Data Protection Officer who is responsible for ensuring the College's compliance with this Policy.

2. About this Policy

- 2.1. 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.
- 2.2. It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. Definitions

- 3.1. *College* – Derwentside College
- 3.2. *College Employee* – For the purposes of this policy, any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.
- 3.3. *Controller* – Any entity (e.g., company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it. A common misconception is that the individuals within organisations are the Controllers. This is not the case; it is the organisation itself which is the Controller.
- 3.4. *Data Protection Laws* – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.
- 3.5. *Data Protection Officer* – Our Data Protection Officer is Andrew Jones – IT & Innovation Manager, who can be contacted at: 01207 585900, enquiries@derwentside.ac.uk.

- 3.6. Information Asset Owner – A member of the College’s workforce who has senior responsibility for ensuring that specific Information Assets are handled and managed appropriately. This includes Personal Data and non-personal information that is critical to the College. Information assets can be held in paper as well as electronic formats. Information Assets and their Owners are recorded in the College Information Asset Register.
- 3.7. EEA – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
- 3.8. ICO – the Information Commissioner’s Office, the UK’s data protection regulator.
- 3.9. *Individuals* – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.
- 3.10. *Personal Data* – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and more sensitive types of data such as trade union membership, genetic data, and religious beliefs. These more sensitive types of data are called “Special Categories of Personal Data” and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.
- 3.11. *Processor* – Any entity (e.g., company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually because of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.
- 3.12. *Special Categories of Personal Data* – Personal Data that reveals a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e., information about their inherited or acquired genetic characteristics), biometric data (i.e., information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. College registration as a Data Controller

- 4.1. The College is required to register with the ICO as a Data Controller and to pay a registration fee each year. Details of the College’s registration is published on the ICO’s website:
<https://ico.org.uk/ESDWebPages/Entry/Z6794092>

5. The College’s obligations

- 5.1. To implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with UK Data Protection Laws, and to:
- Ensure that it integrates data protection into its policies and procedures.
 - Ensure the designation of a suitable Data Protection Officer based on professional qualities and the ability to fulfil the responsibilities, referred to below, of the Data Protection Officer.
 - Ensure the Data Protection Officer has direct access to the Board and/or the Principal and Chief Executive Officer.

- Support the Data Protection Officer, providing the resources necessary to fulfill their responsibilities with full independence and allow access to Personal Data and processing operations.
- Ensure that any other tasks and duties assigned to the Data Protection Officer do not result in a conflict of interest relating to the responsibilities of the Data Protection Officer.
- Ensure that Data Protection is reviewed and monitored at Board and Executive Team meetings with a summary report on Data Protection presented annually.

6. Responsibilities

6.1. The Board of the Corporation is responsible for:

- approving the General Data Protection Policy and for ensuring the College is compliant with all aspects of it, including Data Protection Laws and legislation;
- reviewing and monitoring compliance with the General Data Protection Policy.

6.2. The Data Protection Officer is responsible for:

- maintaining an up to date and legally compliant General Data Protection Policy;
- reporting to the Board and providing assurance that the College is compliant with all aspects of the General Data Protection Policy and relevant laws and legislation;
- chairing a GDPR working group to include the Information Asset Owners and other relevant staff to manage GDPR within the College, and to ensure a central, consistent approach and to monitor GDPR compliance;
- day to day responsibility for monitoring compliance with this Policy and with UK Data Protection Laws;
- advising the College on Data Protection matters and informing College employees of their obligations relating to GDPR;
- being the first contact point for managers seeking advice and guidance about the GDPR Policy or making enquiries about its interpretation;
- providing guidance, where required, on the completion of Data Protection Impact Assessments;
- acting as a point of contact for the ICO;
- receiving reports of data incidents and escalating these in a timely manner when required;
- regularly testing and reviewing the privacy measures implemented by the College and conducting periodic reviews and audits to monitor compliance, assigning additional measures when required;
- maintaining a GDPR Risk Register to identify and assess the threats to the processing of Personal Data within the College and review the technical and organisational measures and processes to reduce the impact of the risk;
- supporting the Information Asset Owners to ensure there are up to date, comprehensive Departmental Information Asset Registers;

6.3. Information Asset Owners are responsible for:

- ensuring that all systems, processes, records, and datasets within their business area are compliant with this Policy and UK Data Protection Laws and assess any risks to this compliance;
- having an overview of any processing activities that occur within their business area, including the repositories that hold Personal Data, and ensuring that these are documented in a comprehensive Departmental Information Asset Register;
- reviewing the information assets, they are responsible for and undertaking compliance checks as required to ensure the confidentiality, integrity, and availability of these assets;
- knowing who has access to their information assets, and for what reason. They must understand when and where data is shared with third parties and ensure suitable GDPR contracts and data sharing agreements are in place as required;
- acting as advocates for issues relating to data protection and privacy, including raising awareness, promoting good practice, and challenging poor practice;
- ensuring data protection principles are applied to new systems and business processes, including undertaking Data Protection Impact Assessments as appropriate within their business areas;

- being able to recognise actual or potential security incidents and Data Breaches and consult with the Data Protection Officer on incident management;
- assisting the Data Protection Officer in their duties by consulting with and providing all appropriate information and support, as required by the Data Protection Officer, in a timely manner regarding new developments and issues affecting the use of Personal Data in the College.

6.4. All College Employees are responsible for:

- ensuring they comply with the requirements set out in this policy;
- ensuring they keep all Personal Data that they collect, store, use and come into contact with during the performance of their duties, secure and confidential;
- ensuring that they do not release or disclose any personal data outside the College to any unauthorised third party; or inside the College, to College Employees not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails;
- taking all steps to ensure there is no unauthorised access to Personal Data whether by other College Employees who are not authorised to see such Personal Data or by people outside the College;
- ensuring they do not access any personal information unless they are authorised to do so, and it is a requirement of their role;
- reporting immediately any data incidents, no matter how trivial they may seem, to the Data Protection Officer as per the College Data Breach Notification Policy;
- ensuring that Personal Data is kept in accordance with the College Data Retention Policy and Departmental Information Asset Registers;
- ensuring they undertake Data Protection training as required by the College.

6.5. The Director of Information Services is responsible for the drafting of this Policy and is responsible for ensuring that this document is regularly reviewed and updated.

6.6. All managers are responsible for ensuring that they and their team members follow the requirements set out in this document.

7. Data Protection Principles

7.1. When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant, and limited to what is necessary for the purposes for which it is being processed;
- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purposes for which it is being processed;
- processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures;

7.2. These principles are considered in more detail in the remainder of this Policy.

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

8. Lawful use of Personal Data

8.1. To collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of

several legal grounds.

- Consent – the individual has given clear consent for the College to process their personal data for a specific purpose.
- Contract – the processing is necessary for a contract the College has with the individual or because they have asked the College to take specific steps before entering into a contract.
- Legal obligation – the processing is necessary for the College to comply with the law (not including contractual obligations).
- Vital interests – the processing is necessary for the College to protect someone's life.
- Public task – the processing is necessary for the College to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- Legitimate interests – the processing is necessary for the College's 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 (this cannot apply to public authorities processing data to perform official tasks).

Further information can be found at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

- 8.2. In addition, when the College collects and/or uses special categories of personal data, the College must show that one of several additional conditions is met.
- 8.2.1. The data subject has given explicit consent to the processing of those personal data for one or more specific purposes, except where Union or Member State law provides that the prohibition may not be lifted by the data subject.
- 8.2.2. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- 8.2.3. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- 8.2.4. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have a regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without consent of the data subject.
- 8.2.5. Processing relates to personal data which are manifestly made public to the data subject. Processing is necessary for the establishment, exercise or defence of legal claims whenever courts are acting in their judicial capacity.
- 8.2.6. Processing is necessary for reasons of substantial public interest, based on Union Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
- 8.2.7. Processing is necessary for purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and the services based on Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards.
- 8.2.8. Processing is necessary for reasons of public interest around public health, such as protecting

against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

- 8.2.9. Processing is necessary for archiving purposes in the public interest scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Further information can be found at <https://ico.org.uk/about-the-ico/our-information/safeguards-policy/policy-document-our-processing-of-special-categories-of-personal-data-and-criminal-offence-data/>

- 8.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 8.1 and 8.2.

9. Transparent Processing – Privacy Notices

- 9.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices:

- Privacy Notice – Students and prospective students;
- Privacy Notice – Employees and prospective employees;
- Privacy Notice – Employers;
- Privacy Notice – Visitors;
- Privacy Notice – Clients.

- 9.2. If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

- 9.3. If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College Employees intend to change how they use Personal Data, they must notify the Data Protection Officer. The Data Protection Officer will then assess whether there is an appropriate lawful basis for changing the way in which Personal Data is used and whether the change requires amendments to be made to the privacy notices and any other controls which need to apply.

10. Purpose Limitation

- 10.1. Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see section 9) and as set out in the College's record of how it uses Personal Data.

- 10.2. Where the College originally collects the data based on legitimate interest, contract or vital interests, the personal data can only be used for another purpose after checking whether the new purpose is compatible with the original purpose. When assessing compatibility of purposes, the College will consider:

- Is there a link between the original purpose and the new purpose?
- What is the context in which the data was collected?
- What type and nature of data does it concern? (e.g., sensitive data?)
- What are the possible consequences of further processing for the individual concerned?
- Are there any appropriate safeguards in place, e.g., encryption or pseudonymization?

- 10.3. If the College originally collects the data based on consent or based on a legal obligation, the College will not

further process the data beyond what is allowed by the original consent or the legal provision(s). In this scenario, the College must obtain new consent or define a new legal basis before further processing.

11. Data Minimisation

- 11.1. The College will abide by the data minimisation principle that requires the College to only collect personal data which is truly necessary for the specified processing purposes.
- 11.2. The College will ensure that the personal data being processed will be:
 - adequate and sufficient to properly fulfil the stated purpose;
 - relevant and have a rational link to that purpose;
 - limited to what is necessary so that the College does not hold more data than is needed for that purpose;

12. Data Quality – Ensuring the Use of Accurate, Up-to-Date and Relevant Personal Data

- 12.1. All College Employees that collect and record Personal Data shall ensure that the Personal Data is recorded accurately and is kept 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.
- 12.2. All College Employees that obtain Personal Data from sources outside the College shall 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 Employees to independently check the Personal Data obtained.
- 12.3. To maintain the quality of Personal Data, all College Employees that access Personal Data shall ensure that they review, maintain, and update it to ensure that it remains accurate, up to date, adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g., for legal reasons or that which is relevant to an investigation).
- 12.4. The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College has a Rights of Individuals Policy and a Rights of Individuals 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 those documents.

13. Retention of Personal Data

- 13.1. Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.
- 13.2. The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, 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.
- 13.3. If College Employees 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 Employees have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.
- 13.4. The Departmental Information Asset Registers clearly define each process a department is involved in, what personal data is processed, along with the required storage, retention, and method of disposal of such data.

14. Accountability

- 14.1. The College takes responsibility for complying with the UK GDPR at the highest management level and throughout the organisation. The College maintains evidence of the steps taken to comply with the UK GDPR and has put in place appropriate technical and organisational measures, highlighted in this document, such as:
- adopting and implementing data protection policies (where proportionate);
 - taking a 'data protection by design and default' approach – putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
 - maintaining documentation of the College processing activities;
 - implementing appropriate security measures;
 - recording and, where necessary, reporting personal data breaches;
 - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
 - appointing a Data Protection Officer;
 - adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- 14.2. All College staff will be accountable for the safety and security of all personal data they come into contact with and will ensure that their actions fully take into account the GDPR principles and requirements.

15. Data Security

- 15.1. 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 the Information Security Policy and procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

16. Data Breach

- 16.1. Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens it will constitute a Personal Data breach. In these cases, College employees will be expected to comply with the College's Data Breach Notification Policy. Paragraphs 13.2 and 13.3 provide examples of what constitutes a Personal Data breach.
- 16.2. A Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration, or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen because of action taken by a third party, they can also occur because of something someone internal does.
- 16.3. There are three main types of Personal Data breach which are as follows:
- 16.3.1. Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Employee is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- 16.3.2. Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g., loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

16.3.3. Integrity breach - where there is an unauthorised or accidental alteration of Personal Data.

- 16.4. All data breaches whether potential (near miss) or actual should be reported to the College Data Protection Officer as soon as they become apparent. A standard [reporting template](#) is available via the College GDPR SharePoint pages. This can be accessed from within the college secure environment. Once the template is completed this will automatically trigger a review of the breach and if appropriate, a declaration to the Information Commissioner within the 72-hour reporting deadline.

17. Appointing Contractors Who Access the College's Personal Data

- 17.1. If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.
- 17.2. One requirement of GDPR is that a 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 with both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.
- 17.3. Any contract where an organisation appoints a Processor must be in writing.
- 17.4. You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it, they may get access to your Personal Data. When you appoint a Processor, the College as Controller remains responsible for what happens to the Personal Data.
- 17.5. GDPR requires the contract with a Processor to contain the following obligations as a minimum, to:
- only act on the written instructions of the Controller;
 - not export Personal Data without the Controller's instruction;
 - ensure staff are subject to confidentiality obligations;
 - take appropriate security measures;
 - only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
 - keep the Personal Data secure and assist the Controller to do so;
 - assist with the notification of Data Breaches and Data Protection Impact Assessments;
 - assist with subject access/individual's rights;
 - delete/return all Personal Data as requested at the end of the contract;
 - submit to audits and provide information about the processing;
 - tell the Controller if any instruction is in breach of the GDPR or other EU or Member State data protection law.
- 17.6. In addition, the contract should set out the:
- subject-matter and duration of the processing;
 - nature and purpose of the processing;
 - type of Personal Data and categories of individuals;
 - obligations and rights of the Controller.

18. Individuals' Rights

- 18.1. GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that Colleges plan how they will handle these requests under GDPR. The different types of rights of individuals are reflected in the following sections:
- 18.2. Subject Access Requests

- 18.2.1. Individuals have the right under the GDPR to ask the College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right, but additional information must be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, the College will no longer be able to charge a fee for complying with the request.
- 18.2.2. Subject Access Requests are becoming more and more common and 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.

18.3. Right of Erasure (Right to be Forgotten)

- 18.3.1. 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 ground 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;
 - the Personal Data must be erased for compliance with a legal obligation.
- 18.3.2. 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.

18.4. Right of Data Portability

- 18.4.1. An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format where:
- the processing is based on consent or on a contract;
 - the processing is carried out by automated means.
- 18.4.2. This right isn't the same as subject access and is intended to give individuals a subset of their data.

18.5. The Right of Rectification and Restriction

- 18.5.1. Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

- 18.6. The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws and will ensure that it allows Individuals to exercise their rights in accordance with the College's Rights of Individuals Policy and Rights of Individuals Procedure. All College employees should be familiar with these documents.

19. Marketing and Consent

- 19.1. The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.
- 19.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR will bring about several important changes for organisations that market to individuals, including:
- providing more detail in their privacy notices, including for example whether profiling takes place;

- rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO likes consent to be used in a marketing context.

19.2. The College must also be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply to direct marketing i.e., a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e., calls, emails, texts, faxes. PECR rules apply even if you are not processing any Personal Data.

19.3. Consent is central to electronic marketing. We would recommend that the best practice is to provide an unticked opt-in box.

19.4. Alternatively, the College may be able to market using a "soft opt in" if the following conditions were met:

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

20. Automated Decision Making and Profiling

20.1. Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

20.1.1. 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.

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

20.2. 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 Laws. If College Employees therefore wish to carry out any Automated Decision Making or Profiling College Employees must inform the Data Protection Officer.

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

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

21. Data Protection Impact Assessments (DPIA)

21.1. The GDPR requires the College to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals;
- describe the measures to address the risks.

21.2. A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

21.3. Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

21.4. 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 fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

21.5. Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
- 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;
- systematic monitoring of public areas on a large scale e.g., CCTV cameras.

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

22. Transferring Personal Data to a Country Outside the EEA

22.1. Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

22.2. So that the College can ensure it is compliant with Data Protection Laws College Employees must not export Personal Data unless it has been approved by the Data Protection Officer.

22.3. College Employees must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

23. Relevant Legislation / Regulation

23.1. The following legislation and regulations apply to this policy / procedure:

- General Data Protection Regulation (GDPR) 2018.
- Data Protection Act 2018.
- Freedom of Information Act 2000.
- Human Rights Act 1998 (Article 10, the right to privacy).

24. Related Documents

24.1. The following related documents are relevant to this policy / procedure:

- Data Retention Policy
- Data Breach Notification Policy
- Data Breach Notification Procedure
- Privacy Notice – Students and prospective student
- Privacy Notice – Employees and prospective employees
- Privacy Notice – Employer
- Privacy Notice – Visitor
- Privacy Notice – Client

25. Equality Impact Analysis

- 25.1. To ensure its compliance with The Equality Duty of the Equality Act 2010, the College will consider the impact of its decisions, practices, activities and services on employees, learners and service-users with different protected characteristics.
- 25.2. The impact analysis process seeks to ensure that:
- College decisions, practices, activities and services do not inadvertently disadvantage employees, learners, or service-users;
 - opportunities to foster good relations between people from a variety of backgrounds are identified.
- 25.3. The impact of new policies and procedures will be analysed during their development while existing policies and procedures will be assessed at the time of their review.
- 25.4. The impact analysis is in two parts:
- initial screening to determine whether the policy or procedure has, or has the potential, for a high level of negative impact;
 - full analysis where initial screening indicates that the policy or procedure has the potential for a high level, significant and extensive negative impact and/or may breach anti-discriminatory legislation.
- 25.5. Where appropriate, the College will seek to involve individuals with relevant experience, knowledge and understanding in the impact analysis.
- 25.6. Information gathered in the monitoring process will be used in the impact analysis.
- 25.7. Priorities for action arising from the impact analysis will be established through the Equality, Diversity and Inclusion Committee.
- 26. Review**
- 26.1. This document will be reviewed by the end of July 2026.
- 26.2. The Director of Information Services will undertake this review, taking into account the outcomes of the monitoring process, legislative changes and developments in good practice.
- 26.3. As part of the review, the Director of Information Services will seek and consider the views of the College's employees and the Board of the Corporation.
- 26.4. The outcome of the review will be reported to the Executive Team and the Board of the Corporation as part of the ongoing review of the Policy.

27. Document Identification

Category [select ONE only]	<input type="checkbox"/> Programmes/courses <input type="checkbox"/> Partnerships <input type="checkbox"/> Finance <input type="checkbox"/> Quality <input checked="" type="checkbox"/> Governance <input type="checkbox"/> Health and safety <input type="checkbox"/> Facilities <input type="checkbox"/> Computer Services <input type="checkbox"/> MIS <input type="checkbox"/> Admissions <input type="checkbox"/> Teaching and learning <input type="checkbox"/> Personnel
Audience [select ALL that apply]	<input checked="" type="checkbox"/> Employees <input checked="" type="checkbox"/> Learners <input checked="" type="checkbox"/> Partners <input checked="" type="checkbox"/> Suppliers

EQUALITY IMPACT ASSESSMENT

This form must be completed when drafting a new policy/procedure or amending an existing policy/procedure. It should be completed at the earliest opportunity so any issues can be resolved/mitigated in advance.

POLICY / PROCEDURE DETAILS	
Name of policy / procedure:	General Data Protection Regulations Policy
Version:	Version 3.1
Date of latest version:	29 August 2024
Manager responsible:	Gary Mills – Director of Information Services
Others involved in this EIA:	

ASSESSMENT			
<p><i>What evidence have you used?</i> (This could be internal data, surveys, complaints/grievances or other external quantitative or qualitative research)</p>	<p>The policy outlines that the College is committed to adhering to GDPR regulations and protecting the confidentiality and integrity of personal data. The Public Sector Equality Duty under section 149 of the Equality Act 2010 requires public bodies to have due regard to the need to:</p> <ul style="list-style-type: none"> • Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010; • Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; and • Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. <p>The College GDPR policy does not impose any additional limitations on a data subject's rights and applies to all data subjects irrespective of age, disability, gender re-assignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.</p> <p>There is reason to believe that the strengthening of the College GDPR practices will serve to promote equality. For example, data subjects will benefit from strengthened safeguards in respect of their rights to access personal data held about them. Data subjects will benefit from the ability to confirm personal data is accurately recorded, including by correcting inaccurate or outdated information, and backed by sanctions and penalties available to the Information Commissioner.</p>		
<p>Who have you engaged / consulted with? (This could be individuals, groups, networks or organisations)</p>	<p>The content of the policy is a requirement of data protection law and as such is not subject to College discretion.</p>		
<p>For each protected characteristic, does the evidence show that the policy/procedure...</p>	<p>does not inadvertently disadvantage or discriminate against staff, learners or service users?</p>	<p>actively explores opportunity and fosters good relations between people of different protected groups and backgrounds?</p>	<p>Where 'no' is checked, or concerns have been identified detail them here:</p>
<p>Age (including older and younger people)</p>	<p>Yes <input checked="" type="checkbox"/></p> <p>No <input type="checkbox"/></p>	<p>Yes <input checked="" type="checkbox"/></p> <p>No <input type="checkbox"/></p>	

Disability (including those with physical disabilities, unseen disabilities and mental health issues)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Sex (both men and women)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Gender reassignment or Gender identity (including trans staff and students who have transitioned, are considering transitioning or are in the process of transitioning from one gender to another, and also non-binary staff and students who do not identify with, or reject gender labels)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Marriage and Civil Partnership	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Pregnancy / Maternity (including breastfeeding mothers)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Race and Ethnicity (including nationality, colour, native language, culture and geographic origin)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Religion and belief (including those with no religion or belief)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Sexual orientation (including, but not limited to, gay, lesbian, bisexual, queer and straight staff and learners)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
Intersectionality (although not a protected characteristic itself it's important to consider how characteristics intersect)	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	

ACTION PLANNING		
Issue Identified	Planned or completed remedial action	Person responsible and timeframe


--	--	--

MONITORING AND REVIEW

How will the impact of your policy and procedure be monitored and reviewed once agreed?

Regular meetings, chaired by the College Data Protection Officer (DPO) to be held through the year with College Information Asset Owners (IAO) and other relevant staff to manage GDPR within the College, and to ensure a central, consistent approach and to monitor GDPR compliance. The DPO will maintain the GDPR policy, ensuring it is legally compliant and report to the Board yearly to provide assurance that the College is compliant with all aspects of the General Data Protection Policy and relevant laws and legislation.

AUTHORISATION

	Signature	Date
Manager responsible:		29/08/2024
EIA Panel:		
EIA Committee's Comments if applicable:		