Reaseheath College Data Protection Policy

1. Overview

The College's reputation and operational success depend on the way it manages and protects personal data. Safeguarding the confidentiality, integrity, and availability of personal data is a responsibility shared by all staff, contractors, and partners working with or on behalf of the College.

As a data controller under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the College collects, stores, and uses personal data about its employees, students, suppliers, governors, parents, and visitors. This policy outlines the principles and responsibilities to ensure lawful, fair, and transparent processing in accordance with the law and good practice.

This policy is applicable to all College Personnel and applies to personal data in any format, whether held electronically, in paper form, or otherwise.

This policy:

- Forms part of the College's wider information governance framework;
- Does not form part of any contract of employment;
- May be updated from time to time. The current version will be available on the College intranet and website.

Queries regarding this policy should be directed to the College's Data Protection Officer (DPO), who oversees compliance with this and related data protection practices.

2. About This Policy

This Policy, along with other referenced documents, sets out the basis on which Reaseheath College collects, uses, stores, shares, and otherwise processes personal data. It applies whether the data is collected directly from individuals or provided by third parties, and whether the data is stored electronically, on paper, or by other means.

This Policy applies to all personal data processed by the College, regardless of the format in which it is held or the category of data subject. This includes, but is not limited to, current and former employees, students, applicants, contractors, governors, parents, visitors, website users, and any other identifiable individuals.

This Policy applies to all College Personnel. You must read, understand, and comply with this Policy and complete any mandatory training related to it. It outlines the minimum standards required to ensure the College meets its legal obligations under the UK GDPR, the Data Protection Act 2018, and relevant guidance issued by the Information Commissioner's Office (ICO).

Failure to comply with this Policy may result in disciplinary action and could expose the College to legal or regulatory action.

Related policies, such as the Records Retention Policy, Data Breach Response Plan, and Acceptable Use Policy, support this Policy and provide more detailed guidance on specific topics. All personnel must comply with both this Policy and all related documents.

3. Definitions

For the purposes of this Policy, the following terms have the meanings set out below. These definitions reflect those found in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

- **Automated Decision-Making (ADM):** A decision made solely by automated means without any human involvement that produces legal effects concerning an individual or similarly significantly affects them.
- **Automated Processing:** Processing of personal data by automated means, including profiling, used to evaluate certain personal characteristics such as performance, preferences, health, or location.
- **College:** Reaseheath College, Reaseheath, Nantwich, Cheshire CW5 6DF.
- **College Personnel:** Any individual engaged by the College who has access to personal data, including employees, workers, agency staff, contractors, volunteers, and governors.
- **Consent:** A freely given, specific, informed, and unambiguous indication of a data subject's wishes by which they, by a statement or a clear affirmative action, signify agreement to the processing of their personal data.
- **Controller (Data Controller):** The natural or legal person, public authority, agency, or other body that determines the purposes and means of processing personal data. The College is the controller for personal data it processes about staff, students, and others.
- **Data Protection Impact Assessment (DPIA):** A documented assessment required for processing likely to result in a high risk to individuals' rights and freedoms. DPIAs help identify and mitigate data protection risks before implementation.
- **Data Processor (Processor):** A person or organisation that processes personal data on behalf of the controller, in accordance with written instructions and a data processing agreement.
- **Data Protection Laws:** The UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any applicable data protection legislation in force in the UK, including guidance and codes of practice issued by the Information Commissioner's Office (ICO).
- **Data Protection Officer (DPO):** The person appointed to advise on and monitor compliance with data protection laws and act as a point of contact with the ICO. The College's DPO is Graeme Lavery (email: graemel@reaseheath.ac.uk, Tel: 01270 613225), supported by Robert Brown of Integrity, Cyber Security and Compliance Consultant.

- **Data Subject:** An identified or identifiable living individual to whom personal data relates. This includes students, employees, job applicants, suppliers, governors, and other individuals the College interacts with.
- **Explicit Consent:** A very clear and specific statement of consent required for processing special category data, automated decision-making, or international transfers under specific conditions.
- **ICO:** The Information Commissioner's Office – the UK's independent authority established to uphold information rights and data protection.
- **Legitimate Interests:** One of the six lawful bases for processing personal data under Article 6(1)(f) UK GDPR. It applies where the processing is necessary for the College's or a third party's legitimate interests, except where those interests are overridden by the interests, rights, or freedoms of the data subject. This basis requires a Legitimate Interest Assessment (LIA) to be documented and reviewed periodically.
- **Personal Data:** Any information relating to an identified or identifiable individual. This includes names, contact details, identification numbers, location data, and online identifiers. Personal data includes expressions of opinion and facts and may also include pseudonymised data if re-identification is possible.
- **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- **Privacy Notice:** A statement or document that explains how the College collects, uses, and protects personal data. Privacy notices must be issued when data is collected and kept under review.
- **Processing / Process:** Any operation performed on personal data, including collection, recording, storage, alteration, retrieval, use, disclosure, deletion, or destruction.
- **Pseudonymisation:** The processing of personal data in such a way that it can no longer be attributed to a specific individual without additional information, which is kept separately and subject to technical and organisational safeguards.
- **Special Category Data:** Sensitive personal data requiring additional protection, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life, or sexual orientation.
- **Third Country:** Any country outside the United Kingdom that is not covered by a UK adequacy decision. Transfers of personal data to third countries are only permitted if appropriate safeguards are in place, such as the International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses (SCCs), or Binding Corporate Rules (BCRs).
- **UK IDTA / Addendum:** Mechanisms recognised under UK law for safeguarding international data transfers, replacing the EU's Standard Contractual Clauses (SCCs) post-Brexit.

4. College Personnel's General Obligations

All College Personnel must comply with this Policy, the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act 2018. Compliance with data protection is a shared responsibility and forms part of every individual's role at Reaseheath College.

All College Personnel are responsible for protecting the confidentiality, integrity, and availability of personal data they access or handle in the course of their duties. Personal data must only be accessed, used, shared, or amended where it is necessary and authorised.

Personal data must not be disclosed:

- To anyone outside the College unless there is a lawful basis and appropriate authorisation or contract in place.
- To other College Personnel unless they are specifically authorised and have a legitimate need to access the information.

Personal data must not be shared informally, such as via email, instant messaging, or verbal communication, unless properly authorised and appropriate safeguards are in place.

College Personnel must take appropriate steps to protect personal data, including:

- Ensuring screens are locked when not in use.
- Storing paper records securely.
- Using College-approved systems for data storage and transmission.
- Following College ICT policies and procedures.

Any suspected loss, misuse, or unauthorised access to personal data must be reported immediately to the Data Protection Officer (DPO) in accordance with the College's Data Breach Procedure.

College Personnel must complete any required data protection training and attend refresher sessions as directed.

5. Data Protection Principles

Reaseheath College is committed to processing personal data in accordance with the core principles set out in Article 5 of the UK GDPR. All personal data must be:

- **Lawful, Fair and Transparent** – Processed lawfully, fairly and in a transparent manner in relation to the individual.
- **Purpose Limitation** – Collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.
- **Data Minimisation** – Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy** – Accurate and, where necessary, kept up to date. Inaccurate personal data must be erased or rectified without delay.
- **Storage Limitation** – Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the data is processed.

- **Integrity and Confidentiality (Security)** – Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.
- **Accountability** – The College must be able to demonstrate its compliance with these principles.

These principles apply to all personal data processed by the College, regardless of the method or medium of processing.

All College Personnel are expected to apply these principles in their work, and to refer to the DPO or the College's supporting policies (e.g. the Information Security Policy, DPIA Process, etc) where clarification or guidance is needed.

6. Lawful Use of Personal Data

All processing of personal data must have a lawful basis under Article 6 of the UK General Data Protection Regulation (UK GDPR). Processing must also be fair and transparent in relation to the individual.

Personal data must only be collected, used, shared, or stored where one or more of the following lawful bases apply:

- **Consent** – The individual has given clear and informed consent to the processing of their personal data for a specific purpose.
- **Contract** – The processing is necessary for the performance of a contract with the individual, or to take steps at their request before entering into a contract.
- **Legal Obligation** – The processing is necessary to comply with a legal obligation to which the College is subject.
- **Vital Interests** – The processing is necessary to protect someone's life.
- **Public Task** – The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the College.
- **Legitimate Interests** – The processing is necessary for the purposes of the College's or a third party's legitimate interests, except where those interests are overridden by the rights and freedoms of the individual. A Legitimate Interest Assessment (LIA) must be completed to justify this basis.

Further guidance on each lawful basis can be found in the ICO's online guide: UK GDPR – Lawful Basis for Processing

Where the College processes special category data (such as health data, ethnicity, or sexual orientation), an additional lawful condition under Article 9 UK GDPR must also apply. These include:

- Explicit Consent from the data subject.
- Employment, social security, and social protection law.
- Protection of vital interests.
- Legal claims or judicial acts.

- Substantial public interest.
- Health or social care purposes.
- Archiving, scientific, or historical research in the public interest.

Further guidance is available here: UK GDPR – Special Category Data

The College maintains a Record of Processing Activities (ROPA) to identify and document the lawful basis for each data processing activity. If College Personnel intend to change how personal data is used, they must first consult the Data Protection Officer (DPO) before proceeding, as this may affect compliance, privacy notices, and associated controls.

7. Consent

Consent is one of the lawful bases for processing personal data under the UK GDPR. Where the College relies on consent, it must be a freely given, specific, informed and unambiguous indication of the individual's wishes, signified by a clear affirmative action.

Consent must not be assumed. Silence, pre-ticked boxes, or inactivity do not constitute valid consent. Consent requests must be presented in a clear and intelligible manner, separate from other terms and conditions.

Individuals must be given an easy way to withdraw their consent at any time, and the withdrawal must be honoured promptly. Withdrawal of consent must not impact any processing that took place before it was withdrawn.

Consent must be refreshed periodically where appropriate, especially if the College intends to process the data for a new or different purpose than originally stated.

Explicit consent is required when processing:

- Special category personal data.
- Criminal offence data.
- Data used for automated decision-making that has a legal or significant effect; or
- Certain types of international data transfers.

Whenever explicit consent is required, it must be obtained using a clear written or digital statement that specifically addresses the processing in question. A privacy notice must accompany such requests.

The College must maintain clear records of all consents obtained, including:

- Who gave consent and when.
- What the individual was told at the time.
- How consent was given (e.g. online form, paper signature); and
- Whether and when consent has been withdrawn.

Where consent is not the appropriate legal basis for processing, the College will rely on another lawful ground, as outlined in Section 6. Lawful Use of Personal Data

8. Transparent Processing – Privacy Notices

The UK GDPR requires that individuals are informed about how their personal data will be used, in a clear, transparent, and accessible manner. This is achieved through privacy notices, which must be:

- Written in clear and plain language.
- Tailored to the audience.
- Easily accessible at the point of data collection.

Where the College collects personal data directly from the individual (e.g. staff recruitment, student enrolment, website forms), a privacy notice must be provided at the time of collection. This notice must include:

- The identity of the College (as controller).
- Contact details of the Data Protection Officer (DPO).
- The purposes and lawful basis for processing.
- Any recipients of the data (including third-party processors).
- Retention periods.
- Rights of the individual under UK GDPR.
- How to lodge a complaint with the ICO.
- Whether data will be transferred internationally and under what safeguards.

The College has adopted the following core Privacy Notices, which are kept under review and published on the College website and intranet:

- Privacy Notice - Staff
- Privacy Notice – For Enrolled Students
- Privacy Notice – Prospective Students
- Privacy Notice - Job Applicants
- Privacy Notice - College Governors
- Privacy Notice - Website Visitors and General Enquiries

Where the College receives personal data indirectly (e.g. from referees, agencies, third parties, or public sources), a privacy notice must be provided to the individual within a reasonable period, and no later than one month after receipt of the data. You must also check that the data was collected in a compliant manner by the third party.

If the College intends to change how personal data is used, the individual must be informed before the new processing begins. College Personnel must notify the Data Protection Officer (DPO) before making any such changes so that the relevant privacy notice can be reviewed or updated accordingly.

All privacy notices must be regularly reviewed to ensure they remain accurate, comprehensive, and legally compliant.

9. Data Minimisation

The College must ensure that all personal data collected and processed is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is being processed. This is known as the data minimisation principle under Article 5(1)(c) of the UK GDPR.

College Personnel must only access or process personal data that is strictly required for their specific duties. Access must be restricted based on role and responsibility (the principle of least privilege).

The College must avoid the collection of personal data "just in case" it might be useful in the future. Where possible, data fields should be limited to essential items only.

All forms, systems, and processes that involve collecting personal data (e.g. application forms, surveys, software systems) must be reviewed periodically to ensure that they are collecting only what is necessary for their stated purpose.

Where personal data is no longer required for the original purpose (or any lawful secondary purpose), it must be securely deleted, anonymised, or archived in accordance with the College's Data Retention Policy.

Staff designing or procuring new systems must embed data minimisation principles into the system design and consult with the DPO or IT team where necessary to ensure that new or updated processes align with this principle

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

Under Article 5(1)(d) of the UK GDPR, personal data must be accurate and, where necessary, kept up to date. The College must take all reasonable steps to ensure that inaccurate personal data is corrected or erased without delay.

All College Personnel who collect or handle personal data must ensure:

- That data is recorded accurately at the point of collection.
- That the source of the data (if collected indirectly) is reliable.
- That records are updated as necessary when new or corrected information is received.

Where personal data is obtained from third parties, College Personnel must take reasonable steps to ensure the accuracy of the data and confirm that it is relevant and appropriate for the intended purpose. This does not necessarily require independent verification but does require due care and professional judgement.

All systems and processes should include a mechanism to periodically review and, where necessary, update stored personal data — particularly where it is critical to decision-making (e.g. emergency contacts, student enrolment details, payroll information).

If personal data is identified as inaccurate, incomplete, or out of date, it must be corrected or removed promptly in line with the College's Rights of Individuals Policy and Records Management Procedures.

Individuals have the right to request rectification of inaccurate or incomplete data. These requests must be responded to in a timely and lawful manner and documented appropriately.

Personal data that is retained in its original form for evidential, legal, regulatory, or investigative purposes (e.g. disciplinary records, historical assessments, safeguarding logs) must be clearly marked as such and protected against unauthorised alteration or deletion.
This data may be retained beyond standard retention periods where justified and must not be amended, even if inaccuracies are identified, unless required by law or a regulatory body. Any requests for rectification/retention in such cases must be handled carefully in line with the College's procedures and documented appropriately.

11. Storage Limitation – Personal Data Must Not Be Kept for Longer Than Needed

Under Article 5(1)(e) of the UK GDPR, personal data must be kept no longer than is necessary for the purposes for which it was originally collected and processed.

Personal data must not be retained in a form that permits identification of individuals for longer than necessary. The College must determine and document appropriate retention periods for all categories of personal data it holds.

The College's Data Retention Policy defines the retention periods applicable to different types of data (e.g. student records, HR files, financial records), and must be followed by all College Personnel.

All College systems and filing processes should incorporate features to:

- Flag data that is approaching the end of its retention period.
- Enable secure deletion or anonymisation.
- Prevent unauthorised recovery or access after deletion.

Privacy notices must include clear information about how long personal data will be kept or the criteria used to determine that period.

If College Personnel believe that specific data needs to be kept for longer or shorter than the default retention period (e.g. due to litigation, regulatory inquiry, or safeguarding concerns), they must seek guidance from the Data Protection Officer (DPO) before taking any action.

Routine audits should be carried out to ensure compliance with data retention schedules and to identify any personal data being stored beyond its lawful retention period.

12. Data Security

The College is committed to protecting personal data through appropriate technical and organisational measures that safeguard against unauthorised or unlawful processing, accidental loss, destruction, or damage.

All College Personnel are responsible for handling personal data securely, in line with this Policy and the College's wider IT Security and Acceptable Use Policies.

The College maintains a layered approach to data security, which includes but is not limited to:

- Multi-Factor Authentication (MFA) on critical systems.
- Role-based access controls (RBAC).
- Use of encrypted storage and secure transmission protocols.
- Endpoint protection (e.g. antivirus and device management).
- Regular patching and vulnerability management.
- Secure backups and disaster recovery plans.

Where appropriate, the College uses pseudonymisation or encryption to reduce risk in systems or processes where personal data is especially sensitive or exposed to external parties.

Special attention must be given to protecting special category data, safeguarding it from any form of unauthorised access, use, or disclosure. This includes ensuring such data is only stored in authorised, secure systems.

College Personnel must:

- Lock screens and devices when unattended.
- Avoid storing personal data locally on personal or unencrypted devices.
- Only use College-approved systems and platforms to process personal data.
- Report any suspected loss, theft, or compromise of personal data immediately to the DPO.

The College uses tools such as Microsoft Purview or similar data governance platforms to monitor access, apply data classification, and enforce information protection policies.

Physical security measures (e.g. building access controls, CCTV, secure disposal bins for confidential documents) are also in place to protect personal data stored in paper format.

All staff must complete data security training and comply with associated policies such as:

- The Data Classification Policy
- The Clear Desk Policy
- The Acceptable Use Policy

Staff must not attempt to bypass or disable security measures. Any such action may result in disciplinary proceedings.

13. Data Breach

Under the UK GDPR, a personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes both digital and physical data.

The College takes information security and incident response seriously. All College Personnel must be able to recognise and respond to a potential data breach without delay.

If you know or suspect that a data breach has occurred, you must:

- Report it immediately to the Data Protection Officer (DPO) via the designated reporting channel.

- Preserve any evidence related to the incident.
- Avoid taking unauthorised steps to investigate or resolve the breach yourself.

Examples of personal data breaches include:

- Sending personal data to the wrong recipient.
- Loss or theft of devices or paper files containing personal data.
- Emailing an attachment with the wrong information.
- External systems being compromised (e.g. via phishing, malware, or ransomware).
- Unauthorised access to data by staff or third parties.

The College maintains a Data Breach Response Procedure, which includes:

- Triage and impact assessment by the DPO or designated incident team.
- Determination of whether the breach must be reported to the Information Commissioner's Office (ICO) within 72 hours of discovery.
- Assessment of whether the affected individuals need to be notified.
- Documentation of the breach in the College's Data Breach Log, including investigation outcomes and remedial actions.

All data breaches, regardless of size or severity, must be documented and reviewed. Lessons learned from incidents will inform future improvements to data protection practices and staff training.

Failure to report a breach promptly may result in disciplinary action, and in some cases, regulatory penalties against the College for non-compliance with statutory requirements.

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

Where the College engages a third party to process personal data on its behalf (a Data Processor), it must ensure that appropriate due diligence, contractual safeguards, and ongoing monitoring are in place. The College remains legally responsible for the actions of its processors under UK GDPR.

A Data Processor is any third party that processes personal data under the College's instructions — this includes cloud software providers, IT support firms, outsourced HR or payroll providers, and marketing agencies.

Before appointing a new processor, the College must:

- Conduct data protection due diligence to assess the processor's security practices, compliance credentials (e.g. ISO 27001, Cyber Essentials Plus), incident response capability, and any relevant certifications.
- Ensure the processor has adequate technical and organisational measures to protect personal data.

Processors must be appointed only where a written contract (Data Processing Agreement) is in place, containing the minimum terms required under Article 28 of the UK GDPR, including:

- Processing only on documented instructions from the College.

- Duty of confidentiality for staff handling personal data.
- Appropriate technical and organisational security measures.
- Sub-processor uses only with prior College approval and written agreement.
- Assistance in complying with individual rights and data breach obligations.
- Deletion or return of personal data at the end of the contract.
- Right of audit and provision of compliance information.

The contract must also specify:

- The subject matter, duration, nature and purpose of the processing.
- The types of personal data and categories of data subjects involved.
- The obligations and rights of the College as Controller.

The DPO or designated lead must review all processor contracts and maintain a register of all current processors and agreements.

Processors should be monitored and re-evaluated periodically, especially where they handle high-risk or special category data. This may include contract renewal checks, penetration test reports, or updated data protection questionnaires.

College Personnel must not engage or share personal data with any third-party supplier unless approved by the relevant line manager and the Data Protection Officer.

15. Individuals' Rights

Under the UK GDPR, individuals (data subjects) have a number of rights over their personal data. These rights apply regardless of the format in which the data is held and must be respected by all College Personnel.

Individuals can exercise these rights free of charge and the College must respond to most requests within one calendar month. All requests must be referred immediately to the Data Protection Officer (DPO) upon receipt.

The key rights include:

15.1. Right of Access (Subject Access Request)

Individuals have the right to request:

- Confirmation that their personal data is being processed.
- Access to a copy of their personal data.
- Additional information such as how their data is used, who it is shared with, and how long it will be kept.

This is commonly referred to as a Subject Access Request (SAR). The College must respond within one month, extendable by two months for complex cases. SARs must be logged, tracked, and fulfilled under the oversight of the DPO.

15.2. Right to Rectification

Individuals can request that inaccurate or incomplete personal data is corrected. Where appropriate, supplementary statements may be added to clarify context. If the data is held for legal or evidential reasons and cannot be altered, the College will explain this to the requester.

15.3. Right to Erasure ("Right to be Forgotten")

Individuals may request the deletion of their personal data where:

- The data is no longer necessary for its original purpose.
- They withdraw consent (and no other legal basis applies).
- The data has been unlawfully processed.
- The College is under a legal obligation to erase it.

This right is **not absolute** — erasure may be refused in certain cases (e.g. for legal, safeguarding, or regulatory compliance purposes).

15.4. Right to Restrict Processing

Individuals may request a temporary halt to processing of their data in certain situations (e.g. while its accuracy is being verified or a legal dispute is ongoing). Restricted data must not be used but may still be stored securely.

15.5. Right to Data Portability

Where processing is based on consent or contract and is carried out by automated means, individuals may request that their data be transferred to themselves or another organisation in a structured, commonly used, machine-readable format.

15.6. Right to Object

Individuals have the right to object to:

- Processing carried out in the public interest or under legitimate interests.
- Use of their data for direct marketing purposes (which must stop immediately).
- Processing for scientific, historical, or statistical research (in limited cases).

Objections must be considered carefully and only overridden where strong legitimate grounds exist.

15.7. Rights in Relation to Automated Decision-Making and Profiling

Individuals have the right not to be subject to a decision based solely on automated processing (including profiling) which has a legal or similarly significant effect. This type of processing must only take place with appropriate safeguards in place and must be reviewed by a human.

The College has documented procedures in place to assess, verify, respond to, and record all rights requests. These are managed under the Rights of Individuals Policy and overseen by the DPO.

All College Personnel must be familiar with the types of rights requests and know how to escalate them to the DPO immediately. Delays or inappropriate handling of requests could result in legal or regulatory consequences for the College.

16. Accountability

The accountability principle under Article 5(2) of the UK GDPR requires that the College is not only responsible for complying with data protection principles but must also be able to demonstrate that compliance.

To fulfil this obligation, the College has implemented a comprehensive Information Governance Framework that includes:

- Appointment of a suitably qualified Data Protection Officer (DPO);
- Maintenance of a Record of Processing Activities (ROPA) to document how personal data is collected, used, stored, and shared.
- Adoption and publication of data protection-related policies, procedures, and training programmes.
- Completion of Data Protection Impact Assessments (DPIAs) where required.
- Contractual controls with suppliers and processors, including appropriate due diligence and review.
- Annual reviews and internal audits of data protection practices.
- Timely and effective responses to personal data breaches and rights requests.

All College Personnel are responsible for upholding this accountability framework by:

- Understanding and following this policy and related guidance.
- Completing mandatory data protection training.
- Reporting risks, breaches, or non-compliance promptly to the DPO.
- Keeping records and systems accurate and secure.
- Embedding data protection into project planning, procurement, and system design.

The College recognises that data protection compliance is an ongoing obligation. Policies, procedures, and controls are reviewed regularly and improved in response to:

- Legal or regulatory updates.
- Feedback from audits or incidents.
- Technological or organisational changes.

The DPO will report periodically to senior leadership on the College's compliance status, emerging risks, and continuous improvement actions.

17. Recordkeeping

The College is required under Article 30 of the UK GDPR to maintain up-to-date and accurate records of its data processing activities. These records support accountability, transparency, and effective risk management.

The College maintains a central Record of Processing Activities (ROPA) that includes, but is not limited to:

- The name and contact details of the College and the Data Protection Officer (DPO);
- The purposes of each category of processing.
- The categories of individuals and the types of personal data processed.
- Any recipients of the data, including third-party processors.
- Details of international data transfers and safeguards applied.
- Applicable retention periods.
- A description of technical and organisational security measures in place.

In addition to the ROPA, College departments may maintain local logs or inventories for specific processes, assets, or suppliers, provided these are accurate and updated in coordination with the DPO.

College Personnel must ensure that:

- New or changed processing activities are reported to the DPO.
- The College's systems and documentation accurately reflect how data is used.
- Key activities such as consent collection, subject access requests, DPIAs, and breach incidents are logged appropriately.

The DPO is responsible for overseeing the maintenance and review of the College's ROPA and for ensuring that it reflects the current state of data processing across the organisation.

Failure to maintain accurate and complete records may result in non-compliance with data protection law and could lead to enforcement action by the Information Commissioner's Office (ICO).

18. Training And Audit

The College recognises that effective data protection compliance depends on staff awareness, knowledge, and regular review. As such, training and audit are key components of the College's accountability framework.

18.1. Staff Training

All College Personnel must complete mandatory data protection training as part of their induction and on a refresher basis at least annually.

The training covers key topics such as the UK GDPR principles, lawful bases for processing, individual rights, secure data handling, breach response, and recognising phishing or social engineering attempts.

Additional, role-specific training is provided to staff who work with high-risk data, systems, or third-party suppliers (e.g. HR, IT, Finance).

Completion of training is tracked and reported to the DPO and senior management. Non-compliance may result in restricted access to systems or disciplinary action.

18.2. Audit and Review

The College will carry out regular internal audits of its data protection practices. These may be thematic (e.g. subject access, consent, retention) or departmental.

Audits are coordinated by the DPO and may include checks on:

- Compliance with data protection policies.
- Adherence to privacy notices and DPIAs.
- Supplier contract reviews.
- Physical and technical access controls.
- Evidence of staff awareness and training completion.

Findings from audits will inform improvements to policies, systems, or training materials.

The College may also engage external specialists for independent reviews or to test specific security or compliance controls.

Lessons learned from training feedback, audits, and data protection incidents will be used to improve governance and reduce risk.

19. Marketing And Consent

Where the College carries out marketing activities — including promoting events, courses, or services — it must do so in compliance with both the UK GDPR and the Privacy and Electronic Communications Regulations (PECR).

Marketing includes any communication intended to promote the College's services, events, fundraising, or campaigns, and applies whether sent by email, SMS, phone call, post, or online advertising.

19.1. Lawful Basis for Marketing

- The College must have a lawful basis for all marketing communications.
- For electronic marketing (e.g. emails or SMS), consent is usually required unless the soft opt-in exemption applies.
- For postal marketing, the College may rely on legitimate interests but must always provide an opt-out.

19.2. Consent for Marketing

Consent must be:

- Freely given, specific, informed, and unambiguous.

    - Obtained separately from other terms and conditions.
    - Given via clear affirmative action (e.g. unticked opt-in box).
- Individuals must be informed of their right to withdraw consent at any time and provided with a clear and simple method to do so.

19.3. Soft Opt-In

The College may use the soft opt-in rule (under PECR) where:

- Contact details were collected in the context of a sale or negotiation (e.g. student enrolment or short course signup).
- The marketing is for similar services offered by the College.
- The individual was given the opportunity to opt-out at the time and in every subsequent communication.

19.4. Profiling and Personalisation

Where the College uses profiling (e.g. to tailor email content), individuals must be informed and given the opportunity to object.

19.5. Cookies and Tracking

Where the College operates websites or online services:

- Cookie banners must clearly allow users to opt in to non-essential cookies (e.g. analytics or advertising).
- Consent must be recorded and respected, in line with ICO guidance.

19.6. Recordkeeping

The College will retain evidence of:

- When, how, and by whom consent was given.
- The content of the consent statement at the time.
- Any withdrawal of consent.

Marketing lists must be reviewed and maintained to ensure they remain up to date and that individuals who opt out are promptly removed.

20. Automated Decision Making and Profiling

Under the UK GDPR, individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant consequences for them. This applies to decisions made without any meaningful human involvement.

Examples of automated decision making include:

- System-driven admissions or recruitment rejections based solely on scores or algorithms.
- Credit or risk profiling without human review.
- Automatically denying access to services based on data patterns.

Profiling refers to any form of automated processing that evaluates personal aspects of an individual — such as behaviour, interests, location, or academic performance — to predict outcomes or take action.

20.1. The College's Responsibilities

The College will not carry out any automated decision making or profiling that falls within the scope of Article 22 without:

- Informing individuals that automated decision making is taking place.
- Providing clear information about the logic involved and the potential consequences.
- Ensuring individuals can request human intervention, express their point of view, and challenge the decision.

If such processing is to be introduced in future (e.g. via third-party systems or AI tools), the following steps must be taken:

- A Data Protection Impact Assessment (DPIA) must be conducted.
- Approval must be obtained from the Data Protection Officer (DPO) and appropriate senior managers.
- Controls must be in place to ensure fairness, transparency, and individual rights are protected.

The College currently does not use automated decision making for decisions that have legal or similarly significant effects on individuals. Should this change, affected individuals will be informed and their rights respected.

All College Personnel must consult with the DPO before implementing any system or service involving automated decisions or profiling.

21. Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a structured process used to identify and minimise data protection risks in any new or significantly changed processing activity. DPIAs are a core part of the College's privacy by design and default approach.

Under the UK GDPR, a DPIA is mandatory where processing is likely to result in a high risk to the rights and freedoms of individuals. Examples include:

- Use of new technologies (e.g. AI, automated decision making).
- Large-scale processing of special category data (e.g. health or ethnicity).
- Systematic monitoring of public spaces (e.g. CCTV).
- Significant changes to systems handling personal data (e.g. new student records system, finance platforms).

A DPIA must:

- Describe the nature, scope, context and purpose of the processing.
- Assess necessity and proportionality.
- Identify potential risks to individuals (e.g. misuse, breach, unfair profiling).
- Detail measures to mitigate or eliminate those risks.

All DPIAs must be initiated at the earliest possible stage in the project or procurement process — ideally before any contracts are signed or systems developed.

The Data Protection Officer (DPO**)** must be consulted during every DPIA and is responsible for:

- Advising on methodology and risk evaluation.
- Reviewing and signing off completed DPIAs.
- Determining whether consultation with the **I**nformation Commissioner's Office (ICO) is required (in cases of unmitigated high risk).

A DPIA template is available from the DPO and must be used for all assessments. Completed DPIAs must be logged in the College's DPIA Register and retained for accountability.

Processing must not begin until the DPIA has been reviewed and formally approved. Failure to complete a DPIA where required may result in regulatory enforcement or reputational damage.

College Personnel must consult the DPO if they are unsure whether a DPIA is required.

22. Sharing Personal Data

The College may need to share personal data with third parties in the course of its operations. This must always be done **lawfully, fairly, securely,** and in line with the College's privacy notices and data protection obligations.

Data sharing may occur:

- Internally, between departments or staff members with a legitimate and authorised reason to access the data.
- Externally, with trusted partners, suppliers, regulators, auditors, law enforcement, or other institutions (e.g. universities, funders, placement providers).

Personal data must not be shared unless:

- There is a clear lawful basis for doing so (e.g. public task, contract, legal obligation).
- The sharing is proportionate and limited to what is necessary.
- Appropriate technical and organisational safeguards are in place to protect the data.

Before sharing personal data with an external third party, you must ensure that:

- A suitable data sharing agreement (DSA) or Data Processing Agreement (DPA) is in place, where required.
- The recipient will process the data securely and only for the intended purpose.

- Data minimisation principles are followed — avoid sending full datasets if only partial information is needed.

Where the College acts as a joint controller with another organisation (e.g. in a partnership or consortium), roles and responsibilities must be clearly documented and communicated to data subjects.

Do not share personal data:

- Informally or verbally unless clearly justified and documented.
- By insecure methods (e.g. unencrypted USBs or personal email accounts).
- Without checking whether the individual has been informed of the sharing via the relevant privacy notice.

If a request to share data comes from a third party (e.g. police, social services, legal representatives), you must:

- Verify the request is legitimate.
- Record the basis for sharing or refusal.
- Refer complex or high-risk requests to the DPO.

All staff must refer to the College's Third-Party Data Sharing Procedure (if available) or consult the DPO when in doubt.

23. Transferring Personal Data to a Country Outside the UK

Under UK data protection law, personal data must not be transferred to countries outside the United Kingdom unless appropriate safeguards are in place to ensure that individuals' rights and freedoms are protected.

A "restricted transfer" occurs when personal data is sent or made accessible to:

- A third party located in a country outside the UK (including cloud storage or remote access); or
- A third party within a multinational organisation who accesses the data from outside the UK.

23.1. Transfers are only permitted if one of the following safeguards applies:

- The destination country has been granted an adequacy decision by the UK government (e.g. EEA countries, New Zealand, Japan).
- The College has implemented an approved International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses (SCCs).
- The transfer is covered by Binding Corporate Rules (BCRs) (in multinational group structures).
- A derogation under Article 49 UK GDPR applies (e.g. explicit consent, vital interests, legal claims, substantial public interest), which must only be used in limited and exceptional circumstances.

23.2. Before transferring personal data outside the UK, the College must:

- Identify the lawful basis for the transfer.
- Conduct a Transfer Risk Assessment (TRA) to evaluate the legal and security risks in the destination country.
- Ensure that any third-party recipient agrees contractually to adequate security and data protection terms.
- Consult the DPO to confirm whether additional safeguards are needed or if ICO consultation is required.

Staff must not initiate or approve any international data transfer — including through SaaS platforms, overseas contractors, or cloud providers — without prior review by the DPO.

The College maintains a log of international data transfers to demonstrate accountability and regulatory compliance.

24. Changes To This Data Protection Policy

This Data Protection Policy is reviewed regularly to ensure that it remains up to date with legal requirements, guidance issued by the Information Commissioner's Office (ICO), and the College's operational needs.

The policy will be:

- Formally reviewed at least every year, or sooner if significant changes occur (e.g. updates to UK data protection law, new guidance from the ICO, or material changes in College systems or services).
- Approved by the College's senior leadership or designated governance body.
- Version controlled, with the current version clearly published and accessible on the College website, Staff Intranet, and Student Intranet.

All College Personnel will be notified of any material changes to this policy and may be required to complete refresher training where appropriate.

The latest version supersedes all previous versions. It is the responsibility of all College Personnel to familiarise themselves with the most recent policy and to follow it at all times.

Queries regarding this policy should be directed to the Data Protection Officer (DPO).

Date of issue	November 2021
Lead for Policy	Vice Principal Finance and Resources
Reviewed	November 2025
Next Review	November 2026