Policy: Data Protection Policy

Author	**Associate Principal – Quality, Data & Standards**
Date last reviewed	May 2023
Approval route	College Leadership Team, Board of Directors
Date Approved	16th December 2025
Review cycle	Annually
Date Review Due	November 2026
Contractual or Non-Contractual	Contractual
Location of copies	College SharePoint / Website
Policy version	Version 4

CONTENTS

Introduction

1.1 Definitions and Key Terms

Data Protection Laws: include but not limited to The General Data Protection Regulation (GDPR) (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.

Data Controller: The Data Controller determines how and why personal data is collected and used and is responsible for ensuring compliance with data protection laws (e.g. a company, organisation or person). In this policy it is Franklin Sixth Form College (hereinafter referred to as "the College").

Data Subject: An individual whose personal data is processed by the College.

Individuals: Only living individuals are those who can be identified —either *directly or indirectly*— based on information held by the College. This could include direct identifiers like a name, or indirect details such as gender, job title, and office location that together reveal a person's identity. This applies to employees, students, parents, visitors, prospective students, as well as sole traders and business partnerships.

College Staff: in this Policy include all College employees, Members, Directors, Community Governors, consultants or contractors (not an exhaustive list) that access the College's personal data or works on behalf of the College.

Personal Data: Refers to any information about an individual (as defined above) that identifies them or could identify them when combined with other information the College holds. This applies even in a business context. Examples include names, addresses, and email addresses (including business emails like firstname.surname@abc123.co.uk), as well as IP addresses. It also includes more sensitive types of data such as genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below, which are given extra protection by Data Protection Laws.

Special Categories of Personal Data: include information that reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (such as inherited or acquired genetic characteristics), biometric data (such as facial images or fingerprints), details about physical or mental health, sexual life or sexual orientation, and any criminal record.

These categories are considered more sensitive than standard personal data and are subject to stricter controls under data protection laws.

Processing: Any operation performed on personal data, including collection, storage, modification, and transmission.

Processor: A Processor is any third party (such as a company, organisation, or individual) that processes Personal Data on behalf of a Controller (the College), typically under contract or instruction, often as part of an outsourced service or support arrangement.

Safeguarding: Safeguarding individuals (whether they are the data subject, or otherwise) may require information to be shared with other organisations. This shall be done in compliance with the framework set out in this Policy. The framework shall not impede the necessary sharing of information to safeguard individuals.

Data Protection Officer (DPO): The College's Data Protection Officer is the Associate Principal – Quality, Data & Standards and can be contacted at information.governance@franklin.ac.uk. In the absence of the Associate Principal – Quality, Data & Standards, the Finance Director will review and action enquiries on behalf of the Data Protection Officer.

1.2 Franklin Sixth Form College is committed to protecting the privacy, the confidentiality and integrity of Personal Data (as per definition above in **1.1**) and is a key responsibility of everyone within the College. This Policy sets out the College's approach to ensuring the confidentiality, integrity, and availability of personal data processed by the College.

As a College that collects, uses and stores Personal Data about its students, staff, student and staff applicants, suppliers (sole traders, partnerships or individuals within companies), Trustees, Directors, Community Governors, parents and visitors and other people the College has a relationship with or may need to contact. Information may include, for example, monitor performance, achievements, health and safety which may include in the form of CCTV. It also needs to process information so that College Staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with (this is not an exhaustive list).

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[1] and in particular its obligations under Article 5 of General Data Protection Regulation (GDPR).

The Data Controller determines how and why personal data is collected and used and is responsible for ensuring compliance with data protection laws (e.g. a company, organisation or person). In this Policy it is Franklin Sixth Form College.

The College has implemented this Data Protection Policy to ensure all College Staff[2] 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 a successful working and learning environment for all. College Staff will receive a copy of this Policy when they start and may receive periodic revisions of the Policy.

The Policy does not form part of any member of the College Staff's contract of employment and the College reserves the right to change this Policy at any time. All members of College Staff are obliged to always comply with this Policy. Any failure to follow the Policy can therefore result in disciplinary proceedings.

Any member of College Staff who considers that the Policy has not been followed in respect of personal data about themselves should raise the matter with the designated Data Protection Officer[3] initially. If the matter is not resolved, it should be raised as a formal grievance.

The College and all College Staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy. This Policy outlines what the College expects from others in order for the College to comply with its legal obligations and compliance is mandatory.

If you have any queries concerning this Policy, please contact our Data Protection Officer (DPO), who is responsible for ensuring the College's compliance with this Policy.

2. About this Policy

This Policy, along with the other referenced policies and documents, outlines the principles and practices the College follows when collecting and using Personal Data—whether obtained directly from individuals or received from third parties. It also establishes the rules governing how the College handles, uses, transfers, and stores Personal Data including keeping it secure. It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. Equality Statement

This Policy applies to all College Staff regardless of age, race, disability, religion or belief, gender, sexual orientation, marital or civil partnership status, gender reassignment, pregnancy or maternity, or any other status. All individuals will be treated in a fair and equitable manner recognising any special needs where adjustments can be made. No individual will suffer any form of unlawful discrimination, victimisation, harassment or bullying because of this Policy.

4. Responsibilities

4.1 Everyone who works for or with the College including College Staff are required to comply with this Policy. Everyone working for or on behalf of the College shares responsibility for ensuring that Personal Data is collected, stored, and handled appropriately, and in line with the requirements of the UK GDPR. Each team that handles personal data must ensure that it is handled and processed in line with this Policy and the data protection principles **(See Section 6 for further guidance on the data protection principles)**. The only people able to access data covered by this Policy should be those who need it for their work.

4.2 College Staff must not disclose or share Personal Data in any of the following circumstances:

- Outside the College.
- Within the College, to individuals who are not authorised to access it.
- Without explicit authorisation from their line manager or the Data Protection Officer (DPO). This applies to all forms of communication, including phone calls and emails.

4.3 All College Staff must take all reasonable steps to prevent unauthorised access to Personal Data — whether by other College Staff without proper authorisation or by individuals outside the College. To ensure data remains secure. College Staff must follow best practices, including (but not limited to):

- Using strong, unique passwords for all systems that handle Personal Data, and never sharing passwords with others and enabling Multi Factor Authentication wherever possible.
- Ensuring Personal Data is not disclosed to unauthorised individuals, inside or outside the College.
- Seeking guidance from a line manager or the Data Protection Officer whenever unsure about data protection responsibilities.

Personal data is of no value to the College unless the College can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, if sending data externally via email, this should be password protected.

- Only certain designated College Staff (as designated by the Data Protection Officer) should transfer data offsite. When data is transferred to external agencies then it should be encrypted or secured by using an electronic file system.
- Personal data should never be transferred outside of the European Economic Area (EEA).
- College Staff should not save copies of personal data to their own computers. Always access and update the central copy of any data.

4.4 Additional Responsibilities of all College Staff and Students

- Checking that any information that they provide to the College in connection with their employment or studies is accurate and up to date.
- Informing the College of any changes to or errors in information, which they have provided, i.e. changes of address. They must ensure that changes of address, etc. are notified to Human Resources (College Staff) and Reception (students).
- Reporting known or suspected data breaches to the Data Protection Officer as quickly as possible. The College cannot be held responsible for any such data protection related errors in relation to this Policy or other referenced policies, unless the College Staff member or student has informed the College of them.
- All College Staff and students should keep all data secure, by taking sensible precautions and following the guidelines in this Policy.
- In particular, strong passwords must be used by all and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the College or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.
- All College Staff and students are responsible for ensuring that any use of Artificial Intelligence (AI) tools or systems is appropriate, ethical, and fully compliant with UK Data Protection Law, including ensuring that personal data is not input into AI platforms unless authorised and lawful to do so. **See AI Policy for further guidance.**
- College Staff and students should be aware that Closed-Circuit Television (CCTV) is used and kept for a limited time to help keep everyone safe, and access to footage is restricted to authorised staff who may share it with the police, insurance companies, or exam boards if needed for safety, security, or fraud prevention. **See CCTV Policy for further guidance.**
- Any breach of the UK GDPR and the Data Protection Policy may result in the College's disciplinary procedures being instigated.
- All College Staff are aware from training of their obligations to report any data breaches, however small, immediately to the DPO.
- This is not an exhaustive list and all College Staff and students are responsible for anything else that supports the protection of data for the College and third parties that the College interacts with.

The College will provide regular training to all employees to help them understand their responsibilities when handling data.

4.5 In conjunction with the responsibilities above, the following people have key areas of responsibility:

The Board of Directors is ultimately responsible for ensuring that Franklin Sixth Form College meets its legal obligations in relation to the GDPR.

The College Leadership Team (CLT) is responsible for management of the Data Protection risk within College, and in providing leadership for consistent College-wide adoption of policies and procedures associated with it.

The Data Protection Officer supported by the Head of IT & MIS and their teams is responsible for:

- Keeping The Board of Directors updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this Policy.
- Handling data protection questions from College Staff and anyone else covered by this Policy.
- Dealing with requests from individuals to see the data that the College holds about them (also called 'subject access requests') and any other data subject right.
- Checking and approving any contracts or agreements with third parties that may handle the College's sensitive data.
- Reporting data breaches, when required, to the Information Commissioner's Office (ICO), the UK's data protection regulator.
- Monitoring compliance.
- Maintaining the College ICO Data Protection registration and any other registration requirements, required by the regulator.
- Making recommendations to the College Leadership Team regarding Data Protection/GDPR Policy and good practice.

The Head of IT & MIS is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards. The minimum standards are:
- Cyber Essentials are maintained in terms of requirements and certifications.

This will include the technological measures to:

- Protect against potential data theft, whether on-site or in transit
- Protect against third party deletion or alteration of personal data
- Protect against data loss due to inadequate backups
- Maintain a resilient infrastructure which helps ensure business continuity in the College
- Perform regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluate any third-party services the College is considering using to store or process data. For instance, cloud computing services.
- Monitor compliance and carry out the implementation of the **Franklin Computer & Network User Agreement.**
- Review the **Franklin Computer and Network User Agreement** and related procedures, and implement any other relevant IT and Data Security based policies in line with an agreed schedule.
- Keep up to date and implement any additional security standards to protect the data, systems, services and equipment of the College.
- Site servers containing personal data in a secure location, away from general office space.
- Back up personal data frequently. Those backups should be tested regularly, in line he College's standard backup procedures.
- Protect all servers and computers containing personal data by approved security software and a firewall.

- Ensure that any CCTV footage is used appropriately and in line with the individual's rights. This should be supported by the Premises Manager.
- Ensure that student data is kept as accurate and up to date as possible.
- Ensure the timely returns of data so that the College fulfils its legal obligations.
- Remove/anonymise data from College systems in a timely manner to abide by the need in UK GDPR to keep data no longer than is necessary.
- Ensure that the privacy statements signed by the students at enrolment are up to date and conform to the DfE guidance.
- Monitor compliance and carry out the implementation of the Data Protection Policy in addition to other referenced policies, in conjunction with the Data Protection Officer**.**
- Provide support to the Data Protection Officer with the compliance and implementation of all data protection related policies, procedures and privacy notices.
- This is not an exhaustive list, and the Head of IT & MIS is also responsible for anything else that supports the protection of data for the College and third parties that the College interacts with.

The Associate Principal – School Partnerships and Student Experience is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Monitoring compliance and carry out the implementation of **the Privacy and Electronic Communications Regulation (PECR) Policy.**
- Reviewing the **PECR Policy** and related procedures, in line with an agreed schedule.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other College Staff to ensure marketing initiatives abide by data protection principles.
- Ensuring that all communications internally and externally (including the College website and social media) adhere to data protection guidance and principles.
- Monitoring compliance and carry out the implementation of sections 10.2.1 and 11 of this Policy in addition to other relevant elements of this Policy**.**
- Providing support to the Data Protection Officer with the compliance and implementation of all data protection related policies, procedures and privacy notices.
- This is not an exhaustive list and the Associate Principal – School Partnerships and Student Experience is also responsible for anything else that supports the protection of data for the College and third parties that the College interacts with.

The Human Resource Manager is responsible for:

- Ensuring that staff applicant and College Staff data is kept as accurate and as up to date as possible.
- Ensuring that College Staff are aware of the College Staff Privacy Notice.
- The timely removal/anonymisation of data from College systems to abide by the need in GDPR to keep data no longer than is necessary.
- Ensuring that all College Staff new to the College carry out data protection training.
- Ensuring that all data protection training is recorded.
- Providing support to the Data Protection Officer with the compliance and implementation of all data protection related policies, procedures and privacy notices.
- This is not an exhaustive list, and the HR Manager is also responsible for anything else that supports the protection of data for the College and third parties that the College interacts with.

The Premises Manager is responsible for:

- Monitoring compliance and carry out the implementation of the **CCTV Policy.**
- Reviewing the **CCTV Policy** and related procedures, in line with an agreed schedule.
- Providing support to the Data Protection Officer with the compliance and implementation of all data protection related policies, procedures and privacy notices.
- This is not an exhaustive list, and the Premises Manager is also responsible for anything else that supports the protection of data for the College and third parties that the College interacts with.

All College Managers are responsible for:

- Ensuring they are satisfied with the legality of holding and using the information collected by College Staff in their area.
- Ensuring that the use of personal data complies with all appropriate College policies.
- Ensuring that relevant College Staff they manage undertake GDPR training where required.
- Referring any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer.
- Raising any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this Policy or our legal obligations without delay, in the first instance the Data Protection Officer.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.
- Providing support to the Data Protection Officer with the compliance and implementation of all data protection related policies, procedures and privacy notices.
- This is not an exhaustive list, and all College Managers are also responsible for anything else that supports the protection of data for the College and third parties that the College interacts with.

5. Data Protection Risks

This Policy safeguards the College against key data security risks, including:

- **Breaches of confidentiality**, such as inappropriate disclosure of information, unlocked computer screens, unencrypted data transfers, and insecure sharing of personal data via email or phone.
- **Failure to offer individuals choice** in how their personal data is used by the College.
- **Reputational damage** resulting from unauthorised access to sensitive data, such as through cyberattacks.

6. Data Protection Principles

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 transparently**
- **Collected for specified, legitimate purposes**
- **Adequate, relevant, and limited**
- **Accurate and kept up to date**
- **Kept in a form which permits identification of data subjects for no longer than is necessary**
- **Processed in a manner that ensures appropriate security**

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

Under Article 5(2) of the UK GDPR, the College, as Data Controller, is responsible for complying with

the data protection principles and must be able to demonstrate this compliance. This principle, known as Accountability, is supported by the College's documented policies and procedures, including this Policy and related documentation.

6.1 Processed lawfully, fairly, and transparently Collected for specified, legitimate purposes, Adequate, relevant, and limited (Personal Data):

To lawfully collect and use personal data, the College must ensure that its processing is based on at least one of the legal grounds set out in Article 6 of the UK GDPR. These legal bases include (these are paraphrased):

- **Consent** – the individual has given clear and valid consent for their personal data to be processed for a specific purpose.
- **Contract** – processing is necessary to fulfil a contract with the individual or to take steps at their request before entering into a contract.
- **Legal Obligation** – processing is required to comply with a legal obligation (excluding contractual obligations).
- **Vital Interests** – processing is necessary to protect someone's life.
- **Public Task** – processing is necessary to carry out a task in the public interest or as part of the College's official functions, where there is a legal basis for the task.
- **Legitimate Interests** – processing is necessary for the legitimate interests of the College or a third party, provided these are not overridden by the individual's rights and interests, particularly in the case of children.

More information about Lawful Basis can be found on the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

6.1.1 Data Mapping and Information Asset Register

The College will comply with Article 30 of the UK GDPR by maintaining a record of its processing activities.

See Data Mapping, Information Asset Register, Data Sharing Agreements & Data Protection Impact Assessments Policy for further guidance.

6.2 Processed lawfully, fairly, and transparently, Collected for specified, legitimate purposes, Adequate, relevant, and limited (Special Categories of Personal Data):

There are additional conditions which need to be met in order to use Special Categories of Personal Data. These are set out in Article 9 and are as follows (these are paraphrased):

- Explicit consent
- Employment and social security obligations
- Vital interests
- Necessary for establishment or defence of legal claims
- Substantial public interest; and
- Various scientific and medical issues

The College needs to ensure that for each type of Special Categories of Personal Data it processes, it has established one of the above legal bases for processing it. The following link provides more detail regarding these conditions. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-conditions-for-processing/

The College regularly reviews how it uses Personal Data to ensure compliance with legal obligations. Any proposed changes by College Staff to the use of Personal Data must be reported to the Head of IT & MIS and Data Protection Officer, who will assess whether updates to records or notifications to individuals are required and determine any necessary safeguards.

6.3 Processed lawfully, fairly, and transparently, Collected for specified, legitimate purposes, Adequate, relevant, and limited (Criminal Offence Data):

There are additional conditions which need to be met in order to use Criminal Offence data. These are set out in Schedule 1 of the Data Protection Act 2018. These include, but are not limited to:

- Employment, social security and social protection
- Health or social care purposes
- Public health
- Preventing or detecting unlawful acts
- Preventing fraud
- Safeguarding of children and individuals at risk

The following link provides more detail regarding the conditions for processing Criminal Offence Data. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/criminal-offence-data/#schedule1

The College will ensure that all law enforcement processing of personal data is based on a valid legal basis. Any proposed changes by College Staff to the use of criminal offence data must be reported to the Head of IT & MIS and Data Protection Officer, who will assess whether updates to records or notifications to individuals are required, and determine any necessary controls.

6.4 Privacy Notices

The College ensures that individuals are informed when their personal data is collected and clearly explains how that data will be used and processed and how to exercise their rights. The College has privacy notices for the following individuals:

- Students
- Student Applicants
- Staff
- Staff Applicants
- Parents/Carers
- Community Governors, Directors, Members, The Board of Trustees and Board of Directors
- Visitors of the College

These can be found here: **Franklin Sixth Form College | Policies & Statements**

If the College changes how it uses personal data, individuals may need to be notified. College Staff must inform the Data Protection Officer of any intended changes, who will assess whether updates to privacy notices or additional controls are required.

6.5 Accurate and kept up to date

- The College will only collect and process personal data as necessary for the specific purposes outlined in privacy notices and recorded in the College's data processing records. Personal data must also be accurate and kept up to date.
- Data should be updated as inaccuracies are discovered. For instance, if a stored telephone number is inactive, it should be removed from the systems which it is stored on.
- All College Staff must ensure that any personal data they collect is accurate, current, and limited to what is adequate and necessary for the intended purpose. Data should be stored in as few locations as needed, and unnecessary duplication must be avoided.

- When collecting personal data from external sources, College Staff must take reasonable steps to ensure it is accurate, up to date, and limited to what is necessary. However, College Staff are not required to independently verify this data.
- College Staff accessing personal data must review and update it regularly to maintain accuracy and relevance, except where data must be preserved in its original form for legal or investigative reasons.
- All College Staff are responsible for keeping their own personal details accurate and up to date, and must inform the College of any changes.
- The College is committed to correcting, deleting, or restricting the use of personal data where required under data protection laws. Section 7 outlines individuals' rights and how the College responds to related requests.

6.6 Kept in a form which permits identification of data subjects for no longer than is necessary

- The College must not retain personal data longer than necessary for the purposes for which it was collected.
- Retention periods for different types of personal data, along with the reasons and secure deletion methods, are set out in the College's **Data Retention and Destruction Policy. See Data Retention and Destruction Policy for further guidance.**
- If College Staff believe data should be retained for a shorter or longer period than specified, or have questions about retention practices, they must contact the Head of IT & MIS or Data Protection Officer for guidance.

6.7 Processed in a manner that ensures appropriate security

The College is committed to protecting personal data and has measures in place to prevent unauthorised access, loss, or damage. Security procedures and technologies are in place to protect Personal Data. College Staff must also follow the **Franklin Computer & Network User Agreement**, which supports this Data Protection Policy. If College Staff have any questions or concerns, they must contact the Head of IT & MIS for guidance.

6.8 Data Storage and Security

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, against unauthorised access, accidental loss, destruction or damage.

Storing Data on Paper

Paper records must be kept in secure locations inaccessible to unauthorised individuals.
If electronic data is printed, College Staff must:

- Store documents in locked drawers or filing cabinets when not in use.
- Avoid leaving printouts in unsecured areas, such as on printers.
- Shred documents when no longer needed.

Storing Data Electronically

Electronic data must be protected from unauthorised access, accidental deletion, malicious hacking attempts or cyber threats by:

- Using strong, regularly changed passwords that are not shared.
- Storing data only on approved drives, servers, or cloud services as approved by the Head of IT & MIS.
- Encryption and pseudonymisation.

- Avoiding removable media unless essential; if used, devices must be password protected, securely stored, and data removed when no longer needed.
- Not storing personal data on removable media (like a CD or DVD). If there is any eventuality where this is required, then these should be kept locked away securely when not being used, please seek advice from the Head of IT & MIS where this is required.
- Securely accessing data systems from outside the College using Remote Desktop services or by secure https:// services over the internet means that personal data should never need to be removed from site or saved to offsite computers.
- Ensuring servers are located in secure, restricted areas.
- Backing up personal data frequently and testing backups regularly.
- Never saving personal data directly to laptops, tablets, or mobile phones particular non-College technology.
- Using approved security software and firewalls on all devices storing personal data.

Any questions about this should be directed to the Head of IT & MIS.

7. Data Breaches

The College is committed to maintaining the security of Personal Data. However, despite best efforts, security incidents may still occur. A Personal Data breach involves the unauthorised loss, access, destruction, alteration, or disclosure of Personal Data. In such instances, all College Staff must comply with the Data Breach Notification Procedure set out in **Appendix 1.**

A Personal Data breach is broadly defined as any incident resulting in the accidental or unlawful loss of access to, destruction of, alteration of, or unauthorised disclosure of Personal Data. Breaches may arise from external threats or internal actions.

Personal Data breaches generally fall into one of the following categories:

- **Confidentiality breach** – Unauthorised or accidental access to or disclosure of Personal Data. Examples include: system hacking, accessing data without appropriate authorisation, loss or theft of devices containing data, misdirected correspondence (e.g. letters or emails), or sharing data with unauthorised individuals.
- **Availability breach** – Accidental or unauthorised loss of access to or destruction of Personal Data. Examples include: lost or stolen devices, ransomware attacks, accidental deletion, or failure to restore data from backup.
- **Integrity breach** – Unauthorised or accidental alteration of Personal Data.

The College's Data Breach Procedure **(Appendix 1)** outlines the process for identifying, reporting, and responding to Personal Data breaches, including required timeframes. Any suspected or confirmed breach must be reported immediately in accordance with that procedure or by contacting the Data Protection Officer.

If you suspect a data breach, please consult this procedure and contact the Data Protection Officer immediately at information.governance@franklin.ac.uk

8. Freedom of Information (FOIs) Requests

The College is required by the Freedom of Information Act 2000 and Environmental Information Regulations 2004 to make certain information it holds available to individuals requesting it.
Requests for information to be released under the Freedom of Information Act or Environmental Information Regulations may be made to the College.

The College will endeavour to provide a response to requests as soon as it is able to.

Requests shall be made within the statutory timeframe of 20 working days, excluding bank holidays. **See Freedom of Information Policy for further guidance.**

9. Appointing Contractors who access the College's personal data

When the College engages a contractor who will act as a Processor of its Personal Data, it must conduct appropriate data protection due diligence and have a written contract in place, as required by Data Protection Laws; the College remains responsible for how the Personal Data is handled, even when processed by a third party.

Contracts with Processors must, at a minimum, require them to: act only on the College's written instructions; not transfer Personal Data without permission; ensure College Staff confidentiality; implement appropriate security measures; use sub-processors only with the College's consent and under contract; assist with data security, breach notifications, DPIAs, and individuals' rights requests; delete or return Personal Data at the end of the contract; allow audits and provide processing information; and inform the College if any instruction breaches data protection law. The contract must also specify the processing's subject matter, duration, nature, purpose, types of Personal Data, categories of individuals, and the College's rights and obligations.

Prior to engaging with a Contractor who will process personal data, authorisation is required from the Data Protection Officer before moving forward with the Contractor. Any questions about this should be directed to the Data Protection Officer.

In certain circumstances, the legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the College may disclose requested data. However, we will ensure the request is legitimate, seeking assistance from the Board of Directors and from the College's legal advisers where necessary.

10. Rights of Individuals (Data Subjects)

Data subjects have the following rights under UK GDPR:

10.1 Right to Access (Subject Access Requests (SARs)):

The right to access personal data held by the College. 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 information has to be provided within the timescale of one month (with a possible extension of a further two months if it is a complex request). A fee cannot be charged for complying with the request unless it is deemed to be excessive. **See Appendix 2** that describes the Subject Access Request procedure.

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at information.governance@franklin.ac.uk of what they are specifically requesting.

The College may respond by asking for further information on the SAR before carrying out the request.

If the SAR is manifestly unfounded or excessive, the College may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request. If the College is not going to respond to the SAR because they believe it to be malicious or vexatious, they shall inform the data subject of the reason(s) for not taking action.

10.2 Right to Erasure (Right to be Forgotten):
Individuals have the right to request the deletion of their personal data in the following circumstances:

- The data is no longer needed for its original purpose.
- Consent has been withdrawn and no other legal basis exists.
- The individual objects to the processing and there are no overriding legitimate reasons to continue.
- The data was processed unlawfully.
- Erasure is required to comply with a legal obligation.

10.2.1 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.

10.3 Right to Data Portability:
Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format when:

- The processing is based on consent or a contract.
- The processing is carried out by automated means.

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

10.4 Right to Rectification and Restriction:
Individuals are given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

10.5 Right to be Informed:

- Individuals have the right to be informed about the collection and use of their personal data, in line with the UK GDPR's transparency requirements.
- The College provides Privacy Notices outlining the purpose of data processing, retention periods, and any third parties with whom the data may be shared **(See section 6.4).**

10.6 Right to Restriction of Processing:
Individuals have the right to request the restriction (or "blocking") of the College's processing of their personal data in the following circumstances:

- When they contest the accuracy of the data, for the period needed to verify its accuracy.
- When processing is unlawful, and the individual requests restriction instead of deletion.
- When the College no longer needs the data, but the individual requires it for the establishment, exercise or defence of legal claims.
- When the individual has objected to processing based on the College's legitimate interests, during the period required to assess whether those interests override the individual's rights.

If the restricted data has been shared with third parties, the College must, where possible, inform those parties of the restriction and provide the individual with their identities.

Upon receiving a valid request, the College must restrict processing and confirm this in writing to the individual within one month.

10.7 Right to Object:
Individuals have the right to object to the College's processing of their personal data in the following situations:

- When processing is based on the College's legitimate interests or a task carried out in the public interest, and the individual objects based on their specific circumstances.
- When the College uses the data for direct marketing.
- When processing is for scientific or historical research, or statistical purposes, and the individual objects based on their specific circumstances.

10.8 Right related to Automated Decision-Making including profiling:
The College must respect individuals' rights regarding automated decision-making and profiling. Individuals have the right to:

- Object to automated processing.
- Request an explanation of the decision-making and request intervention if required.

The College will process all personal data in line with individuals' rights under Data Protection Laws and will enable individuals to exercise those rights. **(See Section 12 for further guidance on Automated Decision-Making and Profiling).**

11. Marketing and Consent
The College will sometimes contact individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

Marketing consists of any advertising or marketing communication that is directed to particular individuals. When the College is marketing to individuals, we must ensure that we provide the following:
Sufficient detail in our privacy notices, including for example whether profiling takes place; and

- Rules on obtaining consent are sufficiently strict and require an individual's "clear affirmative action". The ICO require consent to be used in a marketing context.
- Consent is central to electronic marketing. The College will use an un-ticked opt-in box.

Alternatively, the College may use a "soft opt in" when the following conditions are met:

- contact details have been obtained during interest and/or participation with the College including employer, stakeholders, student applicant emails (this is not an exhaustive list).
- the College are marketing its own similar services.
- the College gives the individual a simple opportunity to opt out of the marketing, both when first collecting the details and in every message after that.

The College will adhere to the Privacy and Electronic Communications Regulations (PECR) which sits alongside the Data Protection Act and the UK GDPR. This applies to direct marketing, such as communications 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 when personal data is not being processed. **See PECR Policy for further guidance.**

12. Automated Decision-Making and Profiling
Under Data Protection Laws, specific rules apply to profiling and automated decision-making involving individuals:

- **Automated decision-making** refers to decisions made solely by automated systems, without human involvement, that have legal or significant effects on an individual.
- **Profiling** involves the automated processing of personal data to assess or predict aspects about an individual.

The College may only carry out automated decision-making or profiling if it fully complies with Data Protection Laws. College Staff must inform and obtain approval from the Data Protection Officer before undertaking any such activities.

The College does not engage in automated decision-making or profiling in relation to its employees.

13. Data Protection Impact Assessments (DPIA)

Under the GDPR, data controllers must conduct a risk assessment (a DPIA) for any new service, product, or process involving personal data. This must be done before processing begins, through a Data Protection Impact Assessment (DPIA) which must be obtained from the Data Protection Officer. The DPIA should start as early as possible in the design phase. It is not a ban on using personal data but an evaluation of data-related risks that must be addressed before launching the new service, product, or process. The DPIA is designed to:

- Describe how personal data is collected and used.
- Assess the necessity and proportionality of the processing.
- Identify risks to individuals' rights and freedoms.
- Outline measures to mitigate those risks.

A DPIA is required when processing is likely to pose a high risk to individuals' rights and freedoms. The DPIA template is available from the Data Protection Officer.

If a DPIA reveals unmitigated high risks, the ICO must be consulted.

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.

If a DPIA shows that a web-based service will be used by children, the College will ensure compliance with The Age-Appropriate Design Code (The Children's Code) **(See Section 16 for further).**

Examples of situations requiring a DPIA include (this is not an exhaustive list):

- Large-scale automated decision-making or profiling with substantial effects including legal or similarly significant.
- Artificial Intelligence (AI).
- Extensive processing of Special Categories of Personal Data or criminal offence data.
- Introduction of new IT systems handling large volumes of data.
- Large-scale systematic monitoring, such as CCTV.

All DPIAs must be reviewed and approved by the Data Protection Officer before carrying out a new service, product or process involving personal data.

See Data Mapping, Information Asset Register, Data Sharing Agreements & Data Protection Impact Assessments Policy for further guidance.

14. Data Transfer outside of the UK

- Data Protection Laws strictly regulate the transfer of personal data outside the UK. This includes sending, storing, or accessing personal data abroad. Transfers must be carefully considered when appointing suppliers outside the UK or suppliers with international group companies who may access the data.
- College Staff must not transfer personal data outside the UK without prior approval from the Data Protection Officer.
- The College only transfers personal data internationally in specific cases, such as with the British Council or relevant authorities in students' countries of origin.

15. Data Sharing Agreements (DSA)

A Data Sharing Agreement (DSA) is a formal contract between organisations that outlines the lawful basis, purpose, and terms under which personal data is shared, in compliance with the UK GDPR and Data Protection Act 2018.

Prior to sharing data with an organisation, a Data Sharing Agreement may be required. You must get authorisation from the Head of IT & MIS or Data Protection Officer prior to sharing data with another organisation.
Any questions about this should be directed to the Head of IT & MIS or Data Protection Officer.

See Data Mapping, Information Asset Register, Data Sharing Agreements & Data Protection Impact Assessments Policy for further guidance.

16. The Age-Appropriate Design Code (The Children's Code)

The Children's Code, also known as the Age-Appropriate Design Code (Children's Code/AADC) is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. The College will aim to abide by the code where relevant.

The College recognises that some of its web-based services are likely to be accessed by individuals under 18. In such cases, particular care must be taken to comply with the Age-Appropriate Design Code (Children's Code).
This applies in situations including, but not limited to:

- Online support services such as web portals and College email.
- Processing data for College applications.
- Use of College-developed or officially endorsed apps likely to be accessed by under-18s.
- The College will continue to monitor the use and development of its digital platforms and update examples as needed.

When the College identifies—through a DPIA or other means—that a service is likely to be used by children, we will ensure it is operated in the child's best interests. This includes:

- Protecting children from exploitation, including commercial or sexual abuse.
- Supporting their physical, emotional, psychological, and social development.
- Promoting their health, wellbeing, and ability to form their own identity and views.
- Respecting their rights to freedom of association, play, and expression.
- Meeting the needs of children with disabilities in line with equality legislation.
- Supporting parents in protecting their children's best interests.
- Acknowledging and giving appropriate weight to children's evolving capacity to express their views.

The College will aim to ensure that all relevant principles of the Age-Appropriate Design Code are applied to any web-based service likely to be used by children. These principles are available on the ICO website.

Any questions about the suitability of an online service should be directed to the Head of IT & MIS.

17. Training and Awareness

The College will provide regular training to College Staff on data protection principles and their responsibilities under the UK GDPR. All employees will be required to adhere to data protection practices.

18. Compliance and Monitoring

The College will regularly review its data protection practices and policies to ensure compliance with the UK GDPR and other applicable laws. Internal audits, risk assessments, and data protection impact assessments will be conducted as necessary.

This Policy will be monitored by the College Leadership Team and Board of Directors (TBC) and reviewed annually by the Associate Principal – Quality, Data and Standards. The College reserves the right to change this Data Protection Policy at any time without notice.

19. Policy References

The Data Protection Policy must be used in conjunction with the following documents and when a specific policy has been referenced above. These include:

- Data Retention and Destruction Policy
- Franklin Computer & Network User Agreement
- Privacy and Electronic Communications Regulations (PECR) Policy
- Data Mapping, Information Asset Register, Data Sharing Agreements & Data Protection Impact Assessments Policy
- Privacy Notices (including Students, Student Applicants, Staff, Staff Applicants, Parents/Carers, Community Governors, Directors, Members and Visitors of the College
- Freedom of Information (FOI) Policy
- Freedom of Expression (FOE) Policy
- Closed Circuit Television (CCTV) Policy
- Artificial Intelligence (AI) Policy
- Learner Behaviour and Attendance Policy.

These can be found here: Franklin Sixth Form College | Policies & Statements or please contact the Data Protection Officer for more information on these policies at information.governance@franklin.ac.uk

20. Contact Information

The College as a Board of Directors is the Data Controller under the GDPR, and the College Board of Directors (TBC) is therefore ultimately responsible for ensuring that implementation.
For any questions or concerns about this Data Protection Policy, or to exercise any of the data subject rights outlined in this Policy, please contact:

- **Data Protection Officer (DPO)**

- **Email:** information.governance@franklin.ac.uk
- **Postal Address:** [Data Protection Officer, Franklin Sixth Form College, Chelmsford Avenue, Grimsby, DN34 5BY]

21. Access to the Policy

The Policy will be available via the College's website: Franklin Sixth Form College | Policies & Statements

Appendix 1: Procedure for Handling for Reporting a Data Breach

Purpose:

This procedure outlines the steps staff should take when reporting a data breach. It ensures that all reports are handled in accordance with Data Protection UK law and relevant policies.

All staff are responsible for reporting known or suspected data breaches to the Data Protection Officer as quickly as possible. The College cannot be held responsible for any such errors unless the staff member or student has informed the College of them. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes. If a member of staff or student believes a breach has taken place, they should contact the Data Protection Officer immediately.

Any data breaches must be reported to the Data Protection Officer who will handle the breach, or those appointed by the Data Protection Officer will handle the breach and the Data Breach Log, which must be completed in conjunction with the staff procedure outlined below.

If any College staff member is to report a data breach, this must be emailed to the Information.Governance@franklin.ac.uk or passed onto the Data Protection Officer **immediately** as the College is required to report the data breach within 72 hours to the Information Commissioner's Office (ICO) if the breach is notifiable.

In the event of a data breach, the College will:

- Assess whether the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Notify the Information Commissioner's Office (ICO) within 72 hours if the breach is notifiable.
- Communicate the breach to affected data subjects if required.
- Implement measures to mitigate the impact of the breach and prevent future occurrences.
- Any security incident will be investigated to determine if the breach was a result of human error, a system error or of a malicious nature. Further staff training and revisions to systems may take place as identified following the investigation.

1. **Immediate Detection of the Breach**

- Upon discovering a potential data breach, the first step is to assess the situation. This includes identifying the scope, source, and potential impact of the breach.
- Staff or systems involved in detecting the breach must report it immediately to the Data Protection Officer (DPO) or those appointed by the Data Protection Officer to deal with data breaches.

2. **Initial Containment**

- Once reported, immediate action should be taken to contain the breach and prevent further unauthorised access, alteration, or loss of data.
- This might include isolating affected systems, changing passwords, or restricting access to certain networks or databases.

3. **Notify Key Stakeholders**

- The DPO or the designated person will inform the College Leadership Team about the breach, including any preliminary findings and steps taken to contain it (depending on the seriousness of the breach).
- If necessary, notify the IT team for further investigation and resolution of the breach.

4. Assessment and Documentation of the Breach

- The nature and severity of the breach must be fully assessed. This includes identifying the types of data involved (personal and sensitive), the number of individuals impacted, and how the breach occurred.
  - **Personal data** refers to any information that can be used to identify an individual, either on its own or when combined with other data. This includes things like your name, address, email, or phone number. It doesn't necessarily have to be deeply private, but it's any information that can be linked back to you personally.
  - **Sensitive data**, on the other hand, is a subset of personal data, but it includes more private or confidential information that could cause harm if exposed. This includes things like:
    Racial or ethnic origin
    Political opinions
    Religious or philosophical beliefs
    Health data
    Sexual orientation
    Genetic data
    Biometric data (e.g. fingerprints)
- Document all relevant details such as how, when, and why the breach took place, and any immediate corrective actions taken.

5. Notify Regulatory Authorities (if applicable)

- If the breach involves personal data and it is likely to result in a risk to the rights and freedoms of individuals, the breach must be reported to the Information Commissioner's Office (ICO) or the relevant data protection authority within 72 hours of detection.
- Include all necessary details: the nature of the breach, the categories of affected individuals, the likely consequences, and measures taken to address the breach.

6. Notify Affected Individuals

- If there is a high risk to the affected individuals (e.g., sensitive personal data), inform them as soon as possible. The notification should be clear, concise, and provide information on what steps they can take to protect themselves.
- Offer support and/or provide a dedicated contact for any follow-up questions (where appropriate).

7. Review and Investigation

- If appropriate carry out an internal investigation to fully understand how the breach occurred, whether it was due to human error, a technical vulnerability, or external factors (e.g., cyberattack).
- Identify weaknesses in the current security protocols and take corrective action to prevent future breaches.

8. Implement Corrective Actions

- Based on the findings of the investigation, implement necessary corrective actions. This might include updating security systems, enhancing training for staff, or revising data access policies.
- Ensure that there are improvements in both prevention and detection mechanisms.

9. Monitor for Further Issues

- After resolving the breach, relevant College Managers associated with the breach are to closely monitor the systems and data for any signs of further issues (where appropriate). This may

include routine security audits and ongoing training for employees on data protection best practices.

10. Report to Management

- Once the breach has been contained and the necessary actions have been taken, report the final details to senior management.
- Include an overview of the incident, the response, the outcome, and any lessons learned. Additionally, highlight any recommendations for strengthening data protection measures moving forward.

11. Review and Update Data Protection Policies

- After the breach is resolved, review and update the organisation's data protection policies and procedures to ensure that future breaches are less likely to occur (where appropriate).

Appendix 2: Procedure for Handling a Subject Access Request (SAR)

Staff Procedure for Handling a Subject Access Request (SAR)

Purpose:
This procedure outlines the steps staff should take when receiving a Subject Access Request (SAR). It ensures that all requests are handled in accordance with Data Protection UK law and relevant policies.

Subject Access Requests must only be handled by those appointed by the Data Protection Officer and the Subject Access Request Log must be completed in conjunction with the staff procedure outlined below.

If any College staff member receive a Subject Access Request – these must be emailed to the Information.Governance@franklin.ac.uk or passed onto the Data Protection Officer **immediately** as the College is required to respond to SARs within 30 calendar days from the date the request is received – which includes collating information for the request, which can take a long period of time.

If personal data from that SAR requestor are being processed, the College shall provide the requestor with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (electronic) means (where possible):

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom the personal data have been or will be disclosed.
- Where possible, the retention period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing.
- The right to lodge a complaint with the Information Commissioner's Office (ICO).
- Where the personal data are not collected from the requestor, any available information as to their source.
- Whether or not automated decision making is used and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

1. Acknowledge Receipt of the Request

- Upon receiving a Subject Access Request (SAR), acknowledge receipt of the request within 1-2 working days. This can be done via email or letter and to include the internal SAR reference number in the response, to help track the request.
- Inform the requester that the organisation has received the SAR and will begin processing it promptly.
- Note the date the request was received, as the response must be provided within 30 calendar days.

2. Confirm Identity of the Requester

- Verify the identity of the requester to ensure personal data is not disclosed to unauthorised individuals.
- If necessary, ask for additional information (e.g. proof of identity, such as a passport or utility bill) to confirm the identity of the person making the request.
- Ensure that the information requested pertains to the correct individual.

3. Determine the Scope of the Request

- Clarify the specifics of the SAR if needed. If the request is too vague or unclear, ask the requester for further details on the personal data they are seeking.
- Assess whether the request pertains only to the data that the College holds or if it includes data from third parties external to data held by the College.
- The College reserves the right to pause the SAR response while awaiting clarification from the requestor at any time in line with the Data Use and Access Act 2025.

4. Identify and Locate Relevant Data

- Identify all systems, databases, and physical locations where personal data may be held about the requester.
- Check email records, HR systems, IT and MIS systems, databases, or any other places where personal data is stored.
- Engage relevant departments (e.g. HR, IT, finance) to ensure all relevant data is identified and retrieved.

Colleges are required to conduct only 'reasonable and proportionate' searches when responding to SAR requests – in line with the Data Use and Access Act 2025.

5. Review the Data for Exemptions

- Review the data retrieved to ensure it does not contain any personal data of other individuals or any information that is exempt from disclosure (e.g. legal privilege, confidential information, or data related to ongoing investigations).
- Redact or withhold data where applicable in accordance with GDPR exemptions.

6. Prepare and Provide the Response

Once the data has been gathered and reviewed, compile the information into an easily accessible format (e.g. PDF or printed copy).
Include:

- A description of the personal data held.
- The purposes for processing the data.
- The recipients or categories of recipients who may have received the data.
- If any data is withheld or redacted, provide a clear explanation of why this has been done, referencing the specific exemption relied upon.
- This then must be peer reviewed by those appointed by the Data Protection Officer to ensure the data is relevant and correctly redacted, prior to sending the information to the requestor.

7. Deliver the Data to the Requester

Ensure the response is delivered securely to the requester, either electronically or by post, as per the requester's preference.
If sending by post, use secure delivery methods to prevent loss or unauthorised access.

8. Keep Records of the Process

Maintain a record of the SAR, the actions taken, and the information provided.
Document any communications with the requester and any issues encountered during the process.
This is important for accountability and to comply with legal requirements.

9. Respond Within the 30-Day Limit

Ensure that the full response to the SAR is sent within 30 calendar days of receiving the request.

If more time is needed (e.g. due to the complexity of the request), inform the requester within the 30-day period and provide an estimated timeline.

10. Handle Complaints or Disputes

If the requester is dissatisfied with the response, inform them of their right to lodge a complaint with the College Principal in the first instance and then the Information Commissioner's Office (ICO).

Consider reviewing the request and response internally if there is any dispute and take corrective action if necessary.

11. Review and Update Processes

After completing the SAR process, review the procedure and make any necessary improvements to ensure efficiency and compliance for future requests.

Update any internal policies or staff training to reflect any lessons learned.

By following this procedure, the organisation ensures compliance with the General Data Protection Regulation (GDPR) and handles Subject Access Requests in a structured and lawful manner.