ABBEY COLLEGE IN MALVERN
abbeycollege.co.uk

Data Protection Policy

Related documents include:

This data-protection policy is linked to the college's:

- Online Safety Policy;
- Acceptable Use of ICT Agreements;
- Child Protection and Safeguarding Policies;
- Security Policy;
- Data Breach Procedure;
- Records Retention and Disposal Schedule;
- Privacy Notices for pupils, parents/carers, staff, applicants and visitors;
- Complaints Procedure;
- any relevant AI, filtering and monitoring, CCTV or biometric procedures.

Where there is any apparent inconsistency between this policy and a specific procedure, staff must seek advice from the Principal or DPO / Data Protection Lead. Statutory safeguarding duties and other legal obligations must be observed.

Legal Status:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018, as amended
- The Data (Use and Access) Act 2025, including applicable amendments to data protection legislation.
- The Privacy and Electronic Communications Regulations 2003 (PECR) as amended.
- The Human Rights Act 1998, where applicable to the processing of personal information.
- The Equality Act 2010, where the processing of personal data relates to equality, disability and protected characteristics.
- The Children Act 1989 and Children Act 2004, where applicable to safeguarding and the protection of children,
- The Education Act 2002, where applicable to the College's statutory safeguarding responsibilities.
- The Protection of Freedoms Act 2012, where applicable to the handling of information relating to Disclosure and Barring Service (DBS) checks.
- Relevant statutory guidance and regulatory requirements issued by the Information Commissioner's Office (ICO), the Department for Education (DfE) and the Independent Schools Inspectorate (ISI).

Regulatory bodies: Information Commissioner's Office (ICO); Department for Education (DfE): Independent Schools Inspectorate (ISI)

Note: The College will have regard to subsequent amendments, replacement legislation and updated statutory guidance as they come into force.

Produced by:	BB	Date:	05/05/18	Checked by:	JKS	Date:	13/11/2026	Approved by:	MN	Date:	13/11/2026

Monitoring and Review

- This policy will be subject to continuous monitoring, refinement and audit by the Principal.
- The Principal will undertake a formal annual review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require. This policy will be reviewed no later than November 2026 or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.
- The designated Data Protection Officer (DPO) / Data Protection Lead of Abbey College is the Bursar, Mr Mehran Noor, who can be contacted by telephone on 01684 892300 or by email at bursar@abbeycollege.co.uk.

- This policy will be reviewed no later than **November 2027** or earlier if changes in legislation, regulatory requirements or best-practice guidelines so require.
- **Amendments:** November 2026 – comprehensive annual review; updated for the commencement of relevant provisions of the Data (Use and Access) Act 2025, current DfE school data-protection guidance and ICO guidance; clarified subject access, complaints, automated decision-making, privacy notices, security, surveillance and educational-record access.

This policy applies to the whole college and is publicly available on the Abbey College website and upon request (available in large print or other accessible format if required) may be obtained from the Abbey College Office.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

Contents

- 1. Aims
- 2. Legislation and guidance
- 3. Definitions
- 4. The data controller
- 5. Roles and responsibilities
- 6. Data protection principles
- 7. Collecting personal data
- 8. Sharing personal data
- 9. Subject access requests and other rights of individuals
- 10. Parental requests to see the educational record
- 11. Biometric recognition systems
- 12. CCTV
- 13. Photographs and videos
- 14. Data protection by design and default
- 15. Data security and storage of records
- 16. Disposal of records
- 17. Personal data breaches
- 18. Training
- 19. Monitoring arrangements

1. Aims

Our college aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), as amended, and other applicable legislation.

This policy applies to all personal data, regardless of whether it is in paper or electronic format. It applies to all staff, volunteers, governors, contractors and external organisations or individuals working on behalf of the college. It covers information relating to prospective, current and former pupils; parents and carers; staff and applicants; governors and advisers; visitors; suppliers; and other individuals whose information the college handles.

The college will protect individuals' rights, process information lawfully and fairly, keep information secure, and be able to demonstrate compliance. Data protection requirements do not prevent necessary and proportionate safeguarding action or lawful information sharing to protect children and adults at risk.

2. Legislation and Guidance

This policy is based on the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (DUAA). The DUAA received Royal Assent on 19 June 2025 and its provisions have commenced in stages. The principal data-protection reforms commenced on 5 February 2026; the

statutory requirements for controllers to operate a data-subject complaints process commenced on 19 June 2026. The college will apply the provisions in force at the time of each processing activity or request.

The policy also takes account of:

- the Privacy and Electronic Communications Regulations 2003 (PECR), as amended, including rules governing electronic marketing, cookies and electronic communications;
- the Protection of Freedoms Act 2012 and applicable provisions governing the use of biometric information in schools;
- the Education (Pupil Information) (England) Regulations 2005, where applicable to a school or record within their scope;
- the Human Rights Act 1998, particularly respect for private and family life;
- the Equality Act 2010, where relevant to the processing and accessibility of information;
- the ICO's current guidance, including guidance on accountability, individual rights, subject access requests, data protection by design, security, personal data breaches and surveillance;
- Department for Education (DfE) guidance, Data protection in schools, including its updates published in 2026, and relevant safeguarding and filtering-and-monitoring guidance;
- the college's safeguarding, online safety, acceptable-use, retention, cyber-security and records-management arrangements.

The college will keep this policy and associated privacy notices, records of processing, contracts and procedures under review when legislation, commencement regulations or regulatory guidance changes.

2.1 Data (Use and Access) Act 2025

The DUAA amends aspects of the UK GDPR and DPA 2018. The changes relevant to the college include the following:

Subject access requests: the statutory response period remains one month in the ordinary case, but the DUAA provides a defined method for calculating the period, permits a further two months where necessary because of the complexity or number of requests, and allows the clock to pause where the controller reasonably needs clarification to identify the personal information or processing activities covered by an access request. Any extension or pause must be justified, recorded and communicated as required by law.

- Reasonable and proportionate searches: the college must make reasonable and proportionate searches for personal information. It will assess each request on its facts, considering the nature and scope of the request, the information held, technical issues and the fundamental right of access. The college will not dismiss a request merely because it is broad or inconvenient, and will record the reasons for any search limitation.
- Complaints: since 19 June 2026, the college must have a process for receiving and dealing with data-protection complaints. The college will acknowledge a complaint within 30 days, investigate it appropriately, keep the complainant informed of progress where appropriate, and communicate the outcome without undue delay.
- Automated decision-making: the DUAA changes the rules for certain solely automated decisions. The college will identify and assess any use of automated decision-making or profiling. Where a decision has legal or similarly significant effects, the college will comply with the applicable safeguards,

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

including appropriate information, the ability to make representations, human intervention and the ability to contest the decision. Additional restrictions apply where special-category data is involved.

- Recognised legitimate interests: the DUAA introduces specified recognised legitimate interests for which a conventional balancing test is not required where the statutory conditions are met. The college will only rely on a recognised legitimate interest where the relevant legal requirements are satisfied and documented. Other legitimate-interest processing will continue to require a proper assessment of the college's interests against individuals' rights and freedoms.
- International transfers: the college will apply the amended statutory framework and ensure that any restricted transfer of personal data outside the UK is supported by an applicable adequacy regulation, appropriate safeguards or another lawful transfer mechanism, with any required transfer risk assessment.
- Regulatory oversight: references in this policy to the regulator should be read as references to the Information Commissioner / Information Commission, as applicable under the DUAA transition and current institutional arrangements.

The college will not assume that the DUAA removes the need for lawful, fair and transparent processing, data minimisation, security, accountability or respect for individual rights. The core data-protection principles continue to apply.

2.2 Data protection complaints

A person who is concerned about how the college has handled their personal information may make a complaint directly to the college. The complaint may be made in writing or electronically to the DPO / Data Protection Lead at the contact details in this policy. The college will provide reasonable assistance to anyone who needs an accessible or alternative means of making a complaint. The complaint will be acknowledged within 30 days and investigated without undue delay. The college will explain the outcome and any action taken. A person may subsequently raise the matter with the Information Commissioner / Information Commission, but should first use the college's complaints process as required by the DUAA.

2.3 AI and new technologies

The college will identify where artificial intelligence, automated tools, analytics, filtering and monitoring systems, biometric systems or other new technologies process personal data. Staff must not enter personal, confidential, safeguarding or special-category information into public or unapproved AI systems. Any proposed use involving personal data must be referred to the DPO / Data Protection Lead before adoption. The college will assess purpose, lawful basis, transparency, security, processor arrangements, retention, international transfers and risks to individuals. A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk.

2.4 Marketing and electronic communications

The college will comply with PECR and data-protection requirements when sending marketing communications or using cookies and similar technologies. Consent will be obtained where required. Any reliance on a soft opt-in or charitable-purpose exemption introduced or amended by the DUAA will only be used where the college's legal status and the precise statutory conditions permit it. Every marketing communication will provide a clear and effective means of opting out. The college will maintain and respect suppression lists.

2.5 Further statutory and regulatory references

The college will maintain a current record of processing activities and accessible privacy notices. It will undertake DPIAs for high-risk processing, maintain appropriate processor contracts, assess international transfers, and apply the statutory rules for personal data breaches and individual rights. The DPO / Data Protection Lead will advise the Principal where a legal change requires a revision to this policy or an associated procedure.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable individual. This may include a name, identification number, location data, online identifier, contact details, images, education records or information about physical, physiological, genetic, mental, economic, cultural or social identity.
Special-category personal data	More sensitive personal data requiring additional protection, including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data used for unique identification, health, and a person's sex life or sexual orientation.
Criminal-offence data	Personal data relating to criminal convictions and offences or related security measures. It is subject to additional legal conditions and safeguards.
Processing	Anything done to personal data, such as collecting, recording, organising, storing, adapting, retrieving, consulting, using, disclosing, combining, restricting, erasing or destroying it. Processing may be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and means of processing personal data.
Data processor	A person or organisation that processes personal data on behalf of a controller and under the controller's documented instructions.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration,

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

	unauthorised disclosure of, or access to, personal data.
Biometric data	Personal data resulting from specific technical processing relating to physical, physiological or behavioural characteristics which allow or confirm unique identification, such as fingerprints or facial recognition templates.
Data Protection Impact Assessment (DPIA)	A process to identify, assess and reduce data-protection risks arising from processing that is likely to result in a high risk to individuals' rights and freedoms.
Privacy notice	Information provided to individuals explaining what personal data is collected, why and how it is used, the lawful basis, recipients, retention, rights and contact details.

4. The Data Controller

Abbey College in Malvern Ltd processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore acts as a data controller in relation to the processing for which it determines the purposes and means.

The college is registered with the Information Commissioner's Office / Information Commission as required by law. The college's registration number is ZA223225. The DPO / Data Protection Lead will ensure that the registration and any applicable fee are kept current.

In some circumstances, another organisation may be an independent or joint controller, for example where information is shared with an awarding body, local authority, health provider or government department. The respective responsibilities will be identified and documented where necessary.

5. Roles and Responsibilities

This policy applies to all staff employed by the college and to external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action. Contractors and processors must comply with the relevant contractual requirements.

5.1 Proprietor

The Proprietor has overall responsibility for ensuring that the college complies with its relevant data-protection obligations, has appropriate governance and resources, and receives assurance about the effectiveness of its arrangements.

5.2 Data Protection Officer / Data Protection Lead

The designated DPO / Data Protection Lead is Mehran Noor, the Bursar. The college has designated this role to oversee implementation of this policy, monitor compliance, advise on data-protection obligations, support DPIAs, maintain awareness and act as the first point of contact for individuals and the regulator.

The college will periodically document whether it is legally required to appoint a statutory DPO under Article 37 UK GDPR. A statutory appointment is required where the relevant criteria apply, including where an organisation is a public authority or body, its core activities involve large-scale regular and systematic monitoring, or its core activities involve large-scale processing of special-category or criminal-offence data. If the college does not meet those criteria, it may nevertheless retain a voluntary DPO / Data Protection Lead arrangement. Where the college formally designates a DPO, it will ensure the role has the independence, access, resources and protections required by law and that there is no conflict of interests.

The DPO / Data Protection Lead will provide an annual report of activities, risks, incidents, training and recommendations to the Proprietor and, where relevant, the Advisory Board. The role does not transfer the controller's legal accountability away from the college.

5.3 Principal

The Principal acts as the representative of the data controller on a day-to-day basis and is responsible for ensuring that staff follow this policy and that data-protection considerations are incorporated into college management and safeguarding arrangements.

5.4 All staff

Staff are responsible for:

- collecting, storing, accessing, sharing and processing personal data in accordance with this policy and their role;
- using personal data only where there is a legitimate work-related need and only for authorised purposes;
- keeping information accurate, relevant and secure and reporting inaccuracies where they are identified;
- informing the college of changes to their own personal data where necessary;
- maintaining confidentiality and not discussing personal or safeguarding information where it may be overheard or disclosed inappropriately;
- immediately reporting suspected data breaches, lost devices, misdirected emails, unauthorised access or disclosure to the DPO / Data Protection Lead;
- immediately forwarding to the DPO / Data Protection Lead any subject access request, data-rights request or data-protection complaint, including informal or verbal requests;
- contacting the DPO / Data Protection Lead before introducing new processing, new technology, AI tools, new monitoring, sharing arrangements, privacy notices or processor contracts;
- seeking advice before transferring personal data outside the UK or using personal data on personal devices or unapproved systems.

All staff must complete required training and follow the college's Data Breach Procedure, Online Safety Policy and Acceptable Use requirements.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

6. Data Protection Principles

The UK GDPR is based on data-protection principles with which the college must comply. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary for those purposes (data minimisation);
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of individuals for no longer than is necessary;
- processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The college must also be able to demonstrate compliance with these principles (accountability). This policy, the college's privacy notices, records of processing, retention arrangements, DPIAs, contracts, training records and incident logs form part of that evidence.

7. Collecting Personal Data

7.1 Lawfulness, fairness and transparency

- We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the college can **fulfil a contract** with the individual, or the individual has asked the college to take specific steps before entering into a contract.

- The data needs to be processed so that the college can **comply with a legal obligation.**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so that the college, as a public authority, can perform a task **in the public interest,** and carry out its official functions

- The data needs to be processed for the **legitimate interests** of the college or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps which require use of personal data, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing Personal Data

The college will not normally share personal data with anyone else unless there is a lawful basis and the sharing is fair, necessary and proportionate. Personal data may be shared where:

- there is a safeguarding or welfare concern, or a risk to the safety of a pupil, parent, member of staff or another person;
- the college needs to liaise with another agency, such as a local authority, social care, health service, police, examination body, regulator or another school, and the sharing is lawful and necessary;
- the college's suppliers or contractors need information to provide services, such as IT, educational platforms, payroll, insurance, catering, accommodation, transport or professional support;
- the college is required or permitted by law to disclose information, including for the prevention or detection of crime or fraud, legal proceedings, tax obligations or regulatory requirements;
- the sharing is necessary to respond to an emergency or protect someone's vital interests;
- the information is sufficiently anonymised for research or statistical purposes, or another lawful basis applies.

The college will not routinely seek consent before safeguarding information is shared where another lawful basis applies or where seeking consent could place a child or another person at risk. Decisions to share safeguarding information will be made in accordance with safeguarding law and guidance, recorded appropriately and limited to what is necessary.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

When using suppliers or contractors as processors, the college will:

- carry out proportionate due diligence and appoint only organisations that provide sufficient guarantees of appropriate technical and organisational measures;
- put in place a written controller-processor contract containing the terms required by Article 28 UK GDPR, including documented instructions, confidentiality, security, sub-processors, assistance with rights requests and breaches, audits and deletion or return of data;
- share only the information necessary to provide the service;
- review the supplier's security, access controls, retention, sub-processors, incident response and international data arrangements;
- ensure that any data-sharing or joint-controller arrangement is documented where required.

Where personal data is transferred outside the United Kingdom, the college will first determine whether the transfer is restricted under data-protection law. It will use an applicable UK adequacy regulation, appropriate safeguards (such as the UK International Data Transfer Agreement or UK Addendum, where appropriate), or a permitted statutory exception. It will complete and retain any required transfer risk assessment and provide transparency to individuals. A supplier's overseas location or use of overseas support staff must be considered.

Staff must not use personal email accounts, consumer file-sharing services or unapproved messaging applications to share personal data. Any urgent disclosure must still be made securely and recorded where appropriate.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject access requests

Individuals have the right to make a subject access request (SAR) to obtain access to personal data the college holds about them. A SAR may be made verbally or in writing; it does not have to mention the UK GDPR or use a particular form. Requests received by any member of staff must be forwarded immediately to the DPO / Data Protection Lead.

A person making a SAR is entitled to confirmation as to whether their personal data is being processed and, where it is, access to a copy of that data and the supplementary information required by Article 15 UK GDPR, including:

- the purposes of processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the data has been or will be disclosed;
- where possible, the envisaged retention period or the criteria used to determine it;
- the source of the data, where it was not collected from the individual;
- the existence of rights to request rectification, erasure or restriction, to object, and to complain to the regulator;
- information about relevant automated decision-making and profiling, including meaningful information about the logic involved and the significance and envisaged consequences for the individual;

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

- where applicable, information about appropriate safeguards for transfers outside the UK.

The college may ask for information reasonably necessary to confirm the requester's identity or authority to act for the data subject. It will not routinely demand two forms of identification where one reliable method is sufficient. If identity cannot reasonably be confirmed, the college may delay responding until it is confirmed.

9.2 Children and subject access requests

Personal data about a child belongs to the child as the data subject. A parent or carer does not automatically have a right to access a child's personal data. A parent may make a request on a child's behalf where the child lacks sufficient understanding to exercise the right themselves, where the parent is otherwise authorised to act, or where the child has given valid authority. The college will consider the child's age, maturity, understanding, wishes, the nature of the information, confidentiality and the child's best interests on a case-by-case basis.

There is no fixed age at which every child is automatically considered capable or incapable of exercising their rights. The college will not rely on a blanket age rule. Where a child is capable of understanding the request and its implications, their own decision and rights will normally take precedence.

9.3 Responding to subject access requests

The college will respond without undue delay and within one month of the relevant starting point under Article 12A UK GDPR, as amended by the DUAA. The applicable period normally begins when the college receives the request. Where the college reasonably requires information to confirm identity or authority, or reasonably requires clarification to identify the personal information or processing activities covered by the request, the statutory calculation may be affected as provided by law.

Where clarification is reasonably required to identify the information or processing activities covered by a SAR, the college may ask the requester for further information. The clock pauses from the day the clarification request is made until the day the information is received. Clarification will not be requested routinely or simply to narrow a request that the college can reasonably search. The college will explain what is needed and record why it is reasonably required.

Where necessary because of the complexity or number of requests, the college may extend the response period by up to a further two months. It must notify the requester within the first month and explain the reasons for the extension.

The college will normally provide the information free of charge. A reasonable fee may be charged, or the college may refuse to act, only where the request is manifestly unfounded or excessive in accordance with the law. The college will be able to demonstrate the reasons for any such decision.
The college will make reasonable and proportionate searches across relevant systems and records. It will consider the scope of the request, the likely location of information, search terms, relevant staff, technical limitations and the burden of reviewing and redacting third-party information. It will not treat a search as disproportionate merely because it is extensive. If the college limits a search, it will document the objective reasons and explain its approach.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

The college will consider exemptions and restrictions carefully. Information may be withheld where a statutory exemption applies, including where disclosure would identify another individual without a lawful basis, where a specific education or safeguarding exemption applies, or where disclosure would be likely to cause the serious harm specified by law. Safeguarding information will not automatically be withheld or disclosed; each item will be assessed against the relevant legal test and the rights and welfare of the child and others. If a request is refused in whole or part, the college will explain the reasons and the individual's right to complain to the regulator, unless the law prevents it from doing so.

9.4 Other data-protection rights of the individual

In addition to the right to make a SAR and to receive privacy information, individuals may have the right to:

- withdraw consent at any time where processing is based on consent;
- ask the college to rectify inaccurate or incomplete personal data;
- request erasure of personal data in circumstances specified by law;
- request restriction of processing in circumstances specified by law;
- object to processing based on public task or legitimate interests, including certain profiling;
- object at any time to processing for direct marketing;
- request data portability where the statutory conditions apply;
- challenge a decision based solely on automated processing where the relevant legal conditions and safeguards apply;
- complain to the college and, if unresolved, to the Information Commissioner / Information Commission.

These rights are not absolute and may be subject to legal conditions, exemptions or the rights of others. Individuals should submit requests to the DPO / Data Protection Lead. Staff who receive a request must immediately forward it and must not promise that it will necessarily be granted.

9.5 Data-protection complaints

The college will maintain a process for receiving and dealing with data-protection complaints. A complaint may be sent to the DPO / Data Protection Lead by email, letter or another accessible means. The college will acknowledge receipt within 30 days, investigate the matter, make appropriate enquiries, keep the complainant informed of progress where appropriate and communicate the outcome without undue delay. The complaint process is distinct from a SAR or other rights request, although a communication may engage more than one process. The college will identify and handle each element appropriately.

10. Parental Requests to See the Educational Record

Parents and those with parental responsibility may ask the college for information about a pupil's education. The college will consider such requests fairly and promptly, having regard to the pupil's age, maturity, understanding, wishes, welfare and the legal rights of the data subject.

The Education (Pupil Information) (England) Regulations 2005 provide a specific statutory right of access to educational records for the governing body of a school maintained by a local authority and certain non-

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

maintained special schools. The Regulations do not generally apply to an independent school such as Abbey College. Accordingly, the college does not represent the 15-school-day statutory educational-record access procedure as applying to Abbey College.

A parent's request for a pupil's personal data will instead be considered under the UK GDPR and DPA 2018. A parent does not automatically have a right to a child's personal data simply by having parental responsibility. Where a parent is authorised to act for the child, or the child is not competent to exercise the right independently, the college will consider the request in accordance with the law and the child's best interests. The college may provide appropriate educational information to parents as part of its ordinary contractual and pastoral relationship with families, subject to the pupil's rights, confidentiality and safeguarding considerations.

Where another school or organisation makes a lawful request for a pupil's records, the college will consider the request under the applicable legal requirements and safeguarding arrangements and will transfer information securely.

11. Biometric Recognition Systems

Where the college uses pupils' biometric data as part of an automated biometric recognition system, for example to facilitate a cashless catering system in which pupils use fingerprints instead of cash or a PIN, it will comply with the Protection of Freedoms Act 2012 and applicable data-protection law.

Before processing a child's biometric information, the college will provide the required written notification to each parent and obtain the written consent of at least one parent, unless a statutory exception applies. The college will explain what biometric information will be taken, how it will be used, how long it will be retained and how consent may be withdrawn.
The college will not process a pupil's biometric information where the pupil objects or refuses to participate, irrespective of any parental consent. A parent may object or withdraw consent in accordance with the statutory provisions. The college will provide a reasonable alternative method of accessing the relevant service, such as a PIN, card or other non-biometric method, without disadvantage.

Where a pupil or parent withdraws consent or the pupil objects, the college will stop processing the biometric information and securely delete it unless there is another lawful reason to retain it. The college will complete a DPIA before introducing or materially changing a biometric system and will ensure that the system stores biometric templates securely and does not retain raw fingerprint images unnecessarily. Where staff members or other adults use a biometric system, the college will provide appropriate information, identify a lawful basis and obtain consent where consent is the appropriate basis. An alternative means of access will be available. Any withdrawal or objection will be handled in accordance with the applicable law.

12. CCTV

The college uses CCTV in various locations around the college site to help maintain a safe and secure environment, protect pupils, staff and visitors, and assist in the prevention and investigation of incidents. CCTV will be operated lawfully, fairly, transparently and proportionately, in accordance with the UK GDPR, DPA 2018 and current ICO guidance on video surveillance.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

The college does not generally need to obtain consent from every person captured by CCTV where another lawful basis applies. It will make people aware that CCTV is in operation through prominent signs and appropriate privacy information. Signs will identify the purpose of the system and provide contact details or a means of obtaining further information.

Cameras will be positioned to achieve legitimate purposes and will not be installed in areas where individuals have a heightened expectation of privacy, such as toilets, changing rooms or private accommodation, except where a highly exceptional and legally justified arrangement has been assessed and approved. Audio recording will not be used unless specifically justified, necessary, proportionate and approved following a DPIA.

Access to CCTV footage will be restricted to authorised personnel. Footage will be retained only for as long as necessary for the purpose for which it was collected, subject to any requirement to preserve evidence of an incident or comply with a lawful request. Requests for footage from individuals, parents, police or other bodies will be referred to the Principal and DPO / Data Protection Lead and assessed under the relevant legal requirements, including the rights of third parties.

Any new or materially changed CCTV system will be subject to a DPIA where required. The college will maintain appropriate security, access logs, retention arrangements and processor agreements where a third party operates or supports the system.

13. Photographs and Videos

As part of college activities, the college may take photographs and record images of pupils, staff and other individuals. Images are personal data where an individual is identifiable. The college will explain the purposes for which images may be used and identify an appropriate lawful basis for each use.
Where consent is the appropriate lawful basis for taking or using pupil photographs and videos for communications, marketing or promotional materials, the college will obtain and record written consent from parents or carers where appropriate and will also explain the proposed use to the pupil in an age-appropriate way. The college will distinguish between internal educational or operational uses, safeguarding records, and external publicity or marketing. Consent will not be used as a blanket basis for every image-related activity.

Uses may include:

- within the college on notice boards, college posters, prospectuses and newsletters;
- outside the college by external agencies such as the college photographer, newspapers or campaigns, where authorised;
- online on the college website or official social-media pages, where the relevant lawful basis and permissions have been established;
- internal educational, pastoral, safeguarding, security or administrative purposes, where necessary and lawful.

Consent may be refused or withdrawn at any time where consent is the lawful basis. The college will explain the practical effect of withdrawal. Where practicable, it will stop future use and remove images from channels under its control, but it may not be possible to retrieve printed materials already

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

distributed or copies republished by third parties. Images will not be accompanied by unnecessary personal information that could increase the risk of identification or harm.
Staff must not take photographs or videos of pupils on personal devices or store them in personal accounts unless specifically authorised under a documented college procedure. Images must be transferred to approved college systems and deleted from devices in accordance with that procedure. Staff must observe safeguarding guidance and any pupil-specific restrictions.

14. Data Protection by Design and Default

The college will put measures in place to show that it has integrated data protection into its processing activities, including:

- appointing a suitably competent DPO / Data Protection Lead and ensuring that the role has appropriate authority, access and resources;
- processing only the personal data necessary for each specified purpose and limiting access to those who need it;
- maintaining accurate and accessible privacy notices and records of processing activities;
- completing a DPIA where processing is likely to result in a high risk to individuals' rights and freedoms, including where required before introducing new technologies or materially changing monitoring;
- considering privacy and security at the procurement and design stage of new systems, applications, educational technology and services;
- ensuring that processor contracts and data-sharing arrangements meet legal requirements;
- reviewing lawful bases, special-category conditions, retention periods, access controls and international transfers;
- regularly training staff and keeping a record of attendance;
- regularly reviewing and auditing privacy and security arrangements;
- maintaining procedures for data-subject rights, complaints, personal data breaches and secure disposal.

The college's record of processing activities will include, as appropriate, the categories of individuals and personal data processed, purposes, lawful bases and any additional conditions, recipients, retention periods, transfers outside the UK, processor details and a general description of technical and organisational security measures.

A DPIA will be undertaken before processing likely to result in high risk. This includes, where appropriate, large-scale processing of special-category or criminal-offence data, systematic monitoring, innovative technology, biometric processing, and new filtering or monitoring systems. The DPO / Data Protection Lead will advise on the assessment. If a high risk cannot be reduced sufficiently, the college will seek advice from the regulator before proceeding where required by law.

14.1 AI, automated decision-making and profiling

The college will maintain oversight of AI tools and automated systems that process personal data. No staff member may introduce or use an AI tool for processing personal data without prior approval through the college's data-protection and IT governance arrangements. Personal data, confidential college

information and safeguarding records must not be submitted to public AI services unless expressly authorised and protected by an approved arrangement.

AI-generated outputs must be checked by a competent member of staff. The college will not rely on an AI system as the sole decision-maker for significant decisions about admission, discipline, safeguarding, academic progression, employment or access to services without first obtaining legal advice and ensuring that all statutory requirements and safeguards are met. Meaningful human involvement must be genuine and not a rubber-stamp exercise. Special-category data is subject to additional restrictions.

14.2 Filtering and monitoring

The college's filtering and monitoring arrangements form part of its safeguarding and online-safety responsibilities. Any personal data generated by filtering or monitoring, including device activity, search prompts, alerts, reports, images or communications, will be processed lawfully, proportionately and transparently. Access will be limited to authorised staff, and clear retention and safeguarding procedures will apply.

Privacy information and acceptable-use arrangements will explain what is monitored, why monitoring takes place, who may access alerts or reports and how long the information is kept. The college will review third-party provider privacy notices and contracts. A DPIA will be completed before introducing a new filtering or monitoring system or making significant changes to an existing system.

15. Data Security and Storage of Records

The college will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. Security measures will be appropriate to the nature and sensitivity of the information and the risks involved.
In particular:

- paper-based records and portable electronic devices containing personal data must be kept under lock and key when not in use;
- papers containing confidential personal data must not be left on office or classroom desks, staffroom tables, noticeboards or anywhere else accessible to unauthorised persons;
- personal data must be stored on approved college systems with access controls, appropriate authentication and security protections;
- where personal information needs to be taken off site, it must be safeguarded and transported securely; paper records should be carried in a secure, closed container;
- the use of removable media, including USB sticks, is not permitted unless expressly authorised, encrypted and controlled by the college;
- passwords and authentication must comply with the college's current IT security requirements; multi-factor authentication must be used where provided or required, and passwords must not be shared;
- staff must lock screens when away from devices, use secure networks and avoid accessing sensitive information over public or insecure connections;
- personal data must not be sent to personal email accounts or stored in personal cloud services or messaging applications;

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

- staff, pupils or governors who are specifically authorised to store personal information on personal devices must follow the same or stronger security procedures as for college-owned equipment and the relevant Online Safety Policy and Acceptable Use requirements;
- devices and systems must be kept updated and protected against malware and unauthorised access;
- personal data sent electronically must be checked for correct recipients and attachments; sensitive information should be encrypted or shared through an approved secure method;
- where personal data is shared with a third party, the college will carry out due diligence and take reasonable steps to ensure it is adequately protected.

Access rights will be reviewed when staff change roles or leave the college. Confidentiality obligations continue after employment or engagement ends. Staff must report any suspected compromise immediately and must not attempt to conceal or independently investigate a suspected breach.

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely in accordance with the college's retention schedule and any legal, regulatory, safeguarding, contractual or litigation hold requirements. Personal data that has become inaccurate or out of date will be rectified where appropriate or securely disposed of where it is no longer required.

Paper-based records will be shredded or destroyed using a secure confidential-waste process. Electronic records will be securely deleted or rendered irretrievable, taking account of backups, cloud storage, devices and third-party systems. Where a third party disposes of records on the college's behalf, the college will require sufficient guarantees of compliance and, where appropriate, obtain confirmation of secure destruction.

Staff must not destroy records that may be relevant to a safeguarding matter, complaint, legal claim, investigation, audit or subject access request without first consulting the Principal or DPO / Data Protection Lead.

17. Personal Data Breaches

The college will take all reasonable endeavours to prevent personal data breaches. A personal data breach includes accidental loss or destruction, unauthorised access, disclosure or alteration, or a failure of security that compromises personal data.

Examples in a college context may include, but are not limited to:

- a non-anonymised dataset being published on the college website which identifies pupils;
- safeguarding, medical or SEND information being made available to an unauthorised person;
- the theft or loss of a college laptop, telephone or paper file containing personal data;
- an email containing personal data being sent to the wrong recipient;
- unauthorised access to a pupil information system, staff records or cloud account;
- loss of data through malware, ransomware or a cyber-attack.

All staff must report a suspected or actual breach immediately to the DPO / Data Protection Lead and Principal, using the college's Data Breach Procedure. Staff must preserve relevant evidence, take

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

reasonable steps to contain the incident and follow instructions. They must not delay reporting while attempting to establish whether a breach is reportable.

The college will record all personal data breaches, including those that are not reported to the regulator. The DPO / Data Protection Lead will assess the facts, likely consequences and risks to individuals, determine containment and remedial action, and advise the Principal.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the college will notify the Information Commissioner / Information Commission without undue delay and, where feasible, within 72 hours of becoming aware of it. Where notification is made after 72 hours, reasons for the delay will be provided. Where a breach is likely to result in a high risk to individuals, the college will also communicate the breach to affected individuals without undue delay, unless a statutory exception applies.

The college will cooperate with the regulator, keep a record of its assessment and decisions, and review whether additional training, technical controls or procedural changes are required. Further details are set out in the Abbey College Data Breach Procedure.

18. Training

All staff and governors are provided with data-protection training as part of their induction process. Data protection will also form part of continuing professional development where changes to legislation, guidance or the college's processes make it necessary.

The college will ensure that staff receive refresher training at least every two years and, as a matter of good practice, annually where practicable. Training will include the handling of personal and special-category data, safeguarding information, secure sharing, subject access and other rights requests, complaints, personal data breach reporting, cyber security, use of AI and the college's specific procedures. Staff whose duties involve higher-risk or specialist processing will receive additional role-specific guidance. The college will maintain records of training and follow up where training has not been completed.

19. Monitoring Arrangements

The DPO / Data Protection Lead is responsible for monitoring and reviewing this policy, advising the Principal and reporting significant risks or deficiencies. The Principal will ensure that the policy is reviewed annually and shared with the Proprietor and, where relevant, the Advisory Board.

Monitoring will include, as appropriate, review of the record of processing activities, privacy notices, processor contracts, international transfers, retention and disposal, access permissions, DPIAs, SARs and complaints, breach records, CCTV and biometric arrangements, staff training and the effectiveness of security controls.

The college will document the annual review and any actions arising from it. Deficiencies or weaknesses will be addressed promptly and without delay.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026