



Abbey Gate College

POLICY: Privacy Notice for Website	
Scope	Whole College
Responsibility	Data Protection Officer
Review & Update	March 2023
Governor Approval	James Brown
Board Level Approval	Andrew Grime

CONTENT HYPERLINKS

[Policy Statement \(1\)](#)

[Policy Statement \(2\)](#)

[Key Personnel](#)

[Practice \(1\) – Responsibility for Data Protection](#)

[Practice \(2\) – Lawful Basis for Collecting Data](#)

[Practice \(3\) – Types of Data Processed by the College](#)

[Practice \(4\) – How the College collects Data](#)

[Practice \(5\) – Access to Personal Data & Sharing](#)

[Practice \(6\) – Retention of Personal Data](#)

[Practice \(7\) – Keeping in Touch and Supporting the College](#)

[Practice \(8\) – Individuals' Rights](#)

[Practice \(9\) – Data Accuracy and Security](#)

[Practice \(10\) – Queries and Complaints](#)

Policy Statement (1)

At Abbey Gate College we are committed to protecting and respecting individuals' privacy and data. This policy is intended to provide information about how the College will use (or "process") personal data about individuals including:

- 1) staff;
- 2) governors;
- 3) current, past and prospective pupils;
- 4) parents, carers or guardians (referred to in this policy as "parents").

Collectively, we refer to these individuals as the College's community.

This information is provided because Data Protection Law gives individuals rights to understand how their data is used. Staff, parents and pupils are all encouraged to read this Privacy Notice and understand the College's obligations to its entire community.

This Privacy Notice applies alongside any other information the College may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This Privacy Notice also applies in addition to the College's other relevant terms and conditions and policies, including:

- 1) any contract between the College and its staff or the parents of pupils;
- 2) the *Data Management Handbook*, including the College's policies on *Mobile Devices*, *Acceptable Use*, *CCTV*, *Retention of Records*;
- 3) the College's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded; and
- 4) the College's IT policies, including online safeguarding policy.

Anyone who works for, or acts on behalf of, the College (including staff, volunteers, governors and service providers) should also be aware of and comply with this Privacy Notice and the College's data protection policy (within the data management handbook for staff, which also provides further information about how personal data about those individuals will be used).

The School DPO Service acts as our data protection provider, including named Data Protection Officer, as below, for Abbey Gate College.

Policy Statement (2)

- 1) This policy applies to all members of the Abbey Gate College community, including those in our EYFS setting.
- 2) Abbey Gate College implements this policy through adherence to the procedures set out in the rest of this document.
- 3) This policy is made available to relevant parties on the College website at www.abbeygatecollege.co.uk. This policy should be read in conjunction with the College's *Data Management Handbook*, *Safeguarding*, *Health and Safety* and *IT policies* as outlined in Policy Statement (1).
- 4) Abbey Gate College is fully committed to ensuring that the application of this policy is in adherence to the General Data Protection Regulation (2018). Further details are available in the College's *Data Management Handbook* policy document.

- 5) Abbey Gate College is fully committed to ensuring that the application of this policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the College's *EDI* policy document.
- 6) This policy is reviewed at least annually, or as events or legislation changes require, by the College Leadership Team and the Governing Body. The deadline for the next review is no later than 12 months after the most recent review date indicated above. Any substantial changes that affect individuals' rights will be provided to them directly as far as is reasonably practicable.
- 7) The most recent updates were made on account of personnel changes.

Key Personnel

- 1) Carole Connelly: Data Protection Officer (DPO – external)
- 2) Helen Goodall: Data Manager
- 3) James Brown: Governor responsible for Data Protection
- 4) Andrew Grime: Chair of Governing Body
- 5) Craig Jenkinson: Head

Practice (1) – Responsibility for Data Protection

Deeside House Educational Trust Ltd (the 'Company') trading as Abbey Gate College is a 'data controller' and gathers and uses certain information about individuals. In this notice, references to 'we' or 'us' mean the Company/College.

The College has appointed the Head as the Privacy Compliance Officer who will deal with all requests and enquiries concerning the College's uses of individuals' personal data (see Practice (8) on 'Individuals' Rights' below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

The Data Protection Officer can be contacted via the College's postal address, by telephone via 01244 332077 (Main Reception) or by email via admin@abbeygatecollege.co.uk.

Practice (2) – Lawful Basis for Collecting Data

In order to carry out its ordinary duties to staff, pupils and parents, the College needs to process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity will need to be carried out in order for the College to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the College's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The College expects that the following uses will fall within that category of its (or its community's) "**legitimate interests**":

- 1) For the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents);

- 2) To provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- 3) To enable access to lessons for students off-site, if they are unable to connect with 'live' transmission. For clarity, lessons delivered through, for example, MS Teams are normally not recorded and are accessible only on a synchronous basis. Any exception to this will be by prior arrangement and authorisation with the member of staff, who will actively enable the 'record' feature.
- 4) Maintaining relationships with alumni and the College community, including direct marketing or fundraising activity;
- 5) For the purposes of donor due diligence, and to confirm the identity of prospective donors and their background and relevant interests;
- 6) For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as tax, diversity or gender pay gap analysis);
- 7) To enable relevant authorities to monitor the College's performance and to intervene or assist with incidents as appropriate;
- 8) To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- 9) To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the College;
- 10) To safeguard pupils' welfare and provide appropriate pastoral care;
- 11) To monitor (as appropriate) use of the College's IT and communications systems in accordance with the College's acceptable use policy;
- 12) To make use of photographic images of pupils in College publications, on the College website and (where appropriate) on the College's social media channels in accordance with the College's policy on taking, storing and using images of children;
- 13) For security purposes, including CCTV in accordance with the College's CCTV policy;
- 14) To carry out or cooperate with any College or external complaints, disciplinary or investigation process; and
- 15) Where otherwise reasonably necessary for the College's purposes, including to obtain appropriate professional advice and insurance for the College.

In addition, the College will on occasion need to process **special category personal data** (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons will include:

- 1) To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for social protection, safeguarding, and cooperation with police or social

- services, for insurance purposes or to caterers or organisers of College trips who need to be made aware of dietary or medical needs;
- 2) To comply with public health requirements in respect of Covid-19 (or similar) testing: including managing on-site testing and/or processing the results of tests taken by pupils or other members of the School community, and sharing this information with relevant health authorities;
 - 3) To provide educational services in the context of any special educational needs of a pupil;
 - 4) To provide spiritual education in the context of any religious beliefs;
 - 5) In connection with employment of its staff, for example DBS checks, welfare, post-employment health questionnaires, union membership or pension plans;
 - 6) To run any of its systems that operate on biometric data, such as for security and other forms of pupil identification (lockers, lunch etc.);
 - 7) As part of any College or external complaints, disciplinary or investigation process that involves such data, for example if there are SEN, health or safeguarding elements; or
 - 8) For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

Practice (3) – Types of Data Processed by the College

This will include by way of example:

- 1) names, addresses, telephone numbers, e-mail addresses and other contact details;
- 2) car details (about those who use our car parking facilities);
- 3) bank details and other financial information, e.g. about parents who pay fees to the College;
- 4) past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- 5) personnel files, including in connection with academics, employment or safeguarding;
- 6) nationality and other immigration status information (eg right to work / study), including copies of passport information;
- 7) where appropriate, information about individuals' health and welfare, and contact details for their next of kin;
- 8) references given or received by the College about staff and pupils, and relevant information provided by previous educational establishments and/or other professionals or organisations working with pupils;
- 9) correspondence with and concerning staff, pupils and parents past and present; and
- 10) images of pupils (and occasionally other individuals) engaging in College activities, and images captured by the College's CCTV system (in accordance with the College's policy on taking, storing and using images of children);

Practice (4) – How the College collects Data

Generally, the College receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases personal data will be supplied by third parties (for example another school, or other professionals or authorities working with that individual); or collected from publicly available resources. Some of the reasons listed above for collecting and using personal information overlap, and there may be several grounds which justify the school's use of individuals' data.

Practice (5) – Access to Personal Data & Sharing

Occasionally, the College will need to share personal information relating to its community with third parties, such as:

- 1) professional advisers (e.g. lawyers, insurers, PR advisers and accountants);
- 2) government authorities (e.g. HMRC, DfE, police or the local authority);
- 3) examination boards; and
- 4) appropriate regulatory bodies (e.g. the Teaching Regulation Agency, the [Independent Schools' Inspectorate](#), the Charity Commission or the Information Commissioner).

For the most part, personal data collected by the College will remain within the College, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- 1) medical records held and accessed only by the College's Lead First-Aider and appropriate medical staff under their supervision, or otherwise in accordance with express consent;
- 2) pastoral or safeguarding files.

The College needs to process such information to comply with statutory duties and to keep pupils and others safe, but the College will ensure only authorised staff can access information on a need-to-know basis. This may include wider dissemination if needed for College trips or for catering purposes. Express consent will be sought where appropriate.

However, a certain amount of any SEND pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care, support and education that the pupil requires.

Staff, pupils and parents are reminded that the College is under duties imposed by law and statutory guidance (including [Keeping Children Safe in Education](#)) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the College's *Safeguarding Policy*.

KCSIE also requires that, whenever a child leaves the school to join another school or college, his or her child protection file is promptly provided to the new organisation. The school will retain a copy in accordance with its retention policy for material related to safeguarding matters.

Finally, in accordance with Data Protection Law, some of the College's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the College's specific directions.

The College works with the following third parties to process personal data:

1. **iSAMS** – this is the main management information system utilised by the College, which contains details such as names, dates of birth, addresses, email addresses and telephone numbers of staff, pupils (past and present), parents / guardians and those listed as emergency contacts, pupils' academic records, and sensitive personal data in relation to pupils' medical records.
2. **Microsoft** – this is one of the main service providers to the college offering a secure cloud-based storage for all college users. Their data access includes (but is not limited to) students names, dates of births, genders, email addresses.
3. **FireFly** – this is the College's virtual learning environment that can be accessed by parents and pupils. The system contains the names, College email addresses and year groups of pupils together with details of their academic record. Parents who set up accounts on the system will need to provide their names and email address.
4. **Parent Pay** - this system enables parents / guardians to pay for non-compulsory items such as trips that are not included on the fee bill. Pupil names and year group data is exported from iSAMS into Parent Pay. Parents must activate their own accounts and provide details such as name and email address in order to be able to use the system. Storage of debit and credit card details is optional. The Schoolcomms element is used for booking after school clubs and activities. The data for that includes pupil name, form, parent name, parent email address and parent telephone number.
5. **Unifrog** – this system holds pupil data to provide a one-stop-shop for finding, comparing and applying for degrees taught in English anywhere in the world. Students activate their own accounts and provide details such as name and email address in order to be able to use the system.
6. **Chartwells Independent** – This is our catering provider, who prepare meals for all students and staff, and are specifically aware of, for example, dietary and medical needs.
7. **GL Assessment** – this system is used for various online academic diagnostic and baseline tests, and pastoral surveys. Student data is exported from iSAMS and imported into GL Assessments. The Personal Data we provide on the platforms relating to Students includes (but is not limited to): Name, age, gender, unique pupil number, assessment results, observations about students' performance in tests, the environment during tests and any other relevant information, for example, any illness of a student prior to or during the testing.
8. **Cambridge CEM** – this online testing platform is used for baseline testing. The Personal Data we provide on the platforms relating to Students includes (but is not limited to): Name, age, gender, unique pupil number, public examination results, assessment results, observations about students' performance in tests, the environment during tests and any other relevant information, for example, any illness of a student prior to or during the testing.
9. **Juniper Education** – SISRA is a software service used to track pupil progress. The Personal Data we provide on the platform relating to Students includes (but is not

limited to): Name, age, gender, unique pupil number, public examination results, assessment results.

10. **UCAS** - The UCAS website is used to make applications to university. During the application process we supply references and predicted grades for individual students to UCAS. The references can include health and family context. The applications are the students' intellectual property but can be viewed by the school.
11. **JCQ Examination boards** – These exams boards are used for GCSE, AS and A Level examinations. As part of the entry process we provide information including (but not limited to) name, age, gender, unique pupil number, SEND access arrangements, and any other relevant information, for example, any illness of a student prior to or during the examination
12. **OS Connect** - College alumni can sign up to use this system in order to be kept informed of relevant news and events, and to keep in contact with fellow alumni. Details such as names, addresses, date of birth and email address are stored by the system.
13. **NHS** – to enable participation in the school vaccination programme we provide pupils names, dates of birth and gender to the local immunisation team.
14. The college invests in several online educational curriculum tools including but not limited to Kerboodle, MathsWatch, Digital Theatre, Doodle, Senaca. As part of the allocation of login information to students we provide them with (as a minimum) student names and college email addresses.

Practice (6) – Retention of Personal Data

The College will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the College.

However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements.

If an individual has any specific queries about how our retention policy is applied, or wishes to request that personal data that they no longer believe to be relevant is considered for erasure, they should please contact the Head. However, please bear in mind that the College will often have lawful and necessary reasons to hold on to some personal data even following such requests.

A limited and reasonable amount of information will be kept for archiving purposes, for example; and even where an individual has requested we no longer keep in touch with them, we will need to keep a record of the fact in order to fulfil their wishes (called a "suppression record").

Practice (7) – Keeping in Touch and Supporting the College

The College will use the contact details of parents, alumni and other members of the College community to keep them updated about the activities of the College, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the College will also:

- 1) Share personal data about parents and/or alumni, if applicable and as appropriate, with organisations set up to help establish and maintain relationships with the College community.
- 2) Contact parents and/or alumni by post and email in order to promote and raise funds for the College and, where appropriate, other worthy causes;
- 3) Should an individual wish to limit or object to any such use, or would like further information about them, they should please contact the Head in writing. An individual always has the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the College is nonetheless likely to retain some of their details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

Practice (8) – Individuals' Rights

Individuals have the following rights:

- 1) to obtain access to, and copies of, the personal data that we hold about them;
- 2) to require us to correct the personal data we hold about them if it is incorrect;
- 3) to require us (in certain circumstances) to erase their personal data;
- 4) to request that we restrict our data processing activities (and, where our processing is based on their consent, they may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal);
- 5) to receive from us the personal data we hold about them which they have provided to us, in a reasonable format specified by them, including for the purpose of them transmitting that personal data to another data controller;
- 6) to object, on grounds relating to their particular situation, to any of our particular processing activities where they feel this has a disproportionate impact on their rights.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply. The school will endeavour to respond to any such requests as soon as is reasonably practicable and in any event within statutory time-limits (which is generally one month, but actually fulfilling more complex or multiple requests, e.g. those involving third party information, may take 1-2 months longer).]

Rights of access, etc.

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the College, and in some cases to ask for it to be erased or amended or have it transferred to others, or for the College to stop processing it – but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Head.

The College will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits (which is one month in the case of requests for access to information, but actually fulfilling more complex requests may take 1 – 2 months longer).

The College will be better able to respond quickly to smaller, targeted requests for information made during term time. If the request for information is manifestly excessive or similar to previous requests, the College may ask the individual to reconsider, or require a proportionate fee (but only where Data Protection Law allows it).

If an individual considers that the personal data we hold on them is inaccurate, they should please let us know. However, the College will not necessarily delete or amend views, opinions, notes or records purely on the request of an individual who disputes the account, although we may keep a record of all parties' viewpoints.

Requests that cannot be fulfilled

Individuals should be aware that the right of access is limited to their own personal data, and certain data is exempt from the right of access. This will include information which identifies other individuals (and parents need to be aware this may include their own children, in certain limited situations – please see further below), or information which is subject to legal privilege (for example legal advice given to or sought by the College, or documents prepared in connection with a legal action).

The College is also not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers), provide examination or other test marks ahead of any ordinary publication, nor share any confidential reference given by the College itself for the purposes of the education, training or employment of any individual.

These exemptions necessarily apply also in the context of teacher-assessed grades, where required in the absence of formal public examinations due to pandemic conditions. Additional details at the time will explain what information will be provided to all relevant pupils, and when, in respect of their grades.

Individuals may have heard of the "right to be forgotten". However, we will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing an individual's (or their child's) personal data: for example, a legal requirement, or where it falls within a legitimate interest identified in this Privacy Notice. All such requests will be considered on their own merits.

Pupil requests

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the College, they have sufficient maturity to understand the request they are making (see section **Whose Rights?** below). A pupil of any age may ask a parent or other representative to make a subject access request on their behalf.

Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the law still considers the information in question to be the child's; for older pupils, the parent making the request may need to evidence their child's authority for the specific request.

Pupils at Senior School are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Slightly younger children may however be sufficiently mature to have a say in this decision, depending on the child and the circumstances.

Parental Requests, etc.

It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The College may consider there are lawful grounds for sharing with or without reference to that pupil.

Parents will in general receive educational and pastoral updates about their children. Where parents are separated, the College will in most cases aim to provide the same information to each person with parental responsibility, but may need to factor in all the circumstances including the express wishes of the child.

All information requests from, on behalf of, or concerning pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

Consent

Where the College is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Examples where we do rely on consent are certain types of uses of images and certain types of fundraising activity. Please be aware however that the College may not be relying on consent but have another lawful reason to process the personal data in question even without an individual's consent.

That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as an alumni or parents' association has been requested).

Whose Rights?

The rights under Data Protection Law belong to the individual to whom the data relates. However, the College will often rely on parental authority or notice for the necessary ways it processes personal data relating to pupils – for example, under the parent contract, or via a form. Parents and pupils should be aware that this is not necessarily the same as the College relying on strict consent (see section on Consent above).

Where consent is required, it may in some cases be necessary or appropriate – given the nature of the processing in question, and the pupil's age and understanding – to seek the pupil's consent. Parents should be aware that in such situations they may not be consulted,

depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

In general, the College will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare. That is unless, in the College's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the College may be under an obligation to maintain confidentiality unless, in the College's opinion, there is a good reason to do otherwise; for example where the College believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the College's acceptable use policy and the College rules. Staff are under professional duties to do the same covered under the relevant staff policy.

Practice (9) – Data Accuracy and Security

The College will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the school office (admin@abbeygatecollege.co.uk) of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law); please see above for details of why the College may need to process an individual's data, or whom an individual may contact if they disagree.

The College will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to College systems. All staff and governors will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

Practice (10) – Queries and Complaints

Any comments or queries on this policy should be directed to the Head using the contact details shown under *Section 1 – Responsibility for Data Protection of this Privacy Policy*.

If an individual believes that the College has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the College's complaints procedure and should also notify the Head. An individual can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the College before involving the regulator.

