



# ABBHEY COLLEGE IN MALVERN

abbeycollege.co.uk

## Abbey College

### Data Protection Policy

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

#### Document Details

Information Sharing Category	Public Domain
Version	V1
Date Published	May 2018
Authorised by (if required)	Principal
Review/Update Date	May 2019
Responsible Area	Senior Leadership and Safeguarding Team

#### Amendments:

Date	Amendment

**Monitoring and Review:** This policy is subject to continuous monitoring, refinement and audit by the Principal. The will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay.

Date Reviewed: May 2018

Date of Next Review: May 2019

Signed:

Mr Malcolm Wood  
Principal

This policy will be reviewed no later than May 2019 or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

The Designated Data Protection Officer of Abbey College is the Bursar, Mr Mehran Noor who can be contacted by phone on: 01684 892300 or email at: bursar@abbeycollege.co.uk

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------

Abbey College in Malvern Ltd (Number 08661073)

Registered in England and Wales. Registered office: 6 Manor Park Business centre, Mackenzie Way, Cheltenham, Gloucestershire, GL51 9TX



## Contents

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

### 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 [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

### 2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data. It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------



### 3. Definitions

Term	Definition
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"><li>Name (including initials)</li><li>Identification number</li><li>Location data</li><li>Online identifier, such as a username</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"><li>Racial or ethnic origin</li><li>Political opinions</li><li>Religious or philosophical beliefs</li><li>Trade union membership</li><li>Genetics</li><li>Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>Health – physical or mental</li><li>Sex life or sexual orientation</li></ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<b>Data controller</b>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<b>Data processor</b>	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
<b>Personal data breach</b>	<p>A breach of security leading to the accidental or unlawful</p>



destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

#### 4. The data controller

Abbey College processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The college is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The college's registration number is ZA223225.

#### 5. Roles and responsibilities

This policy applies to **all staff** employed by our college, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

##### 5.1 Proprietor

The proprietor has overall responsibility for ensuring that our college complies with all relevant data protection obligations.

##### 5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. At Abbey College the DPO is Mehran Noor, the Bursar.

The DPO will provide an annual report of their activities directly to the governing body and, where relevant, report to the board their advice and recommendations on college data protection issues.

The DPO is also the first point of contact for individuals whose data the college processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

##### 5.3 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

##### 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the college of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach – see the Abbey College Data Breach Procedure
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------

*Abbey College is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*



## 6. Data protection principles

The GDPR is based on data protection principles that our college must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the college aims to comply with these principles.

## 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**

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. This will be done in accordance with the [Information and Records Management Society's toolkit for colleges](#).

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------



## 8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## 9. Subject access requests and other rights of individuals

### 9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the college holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------



Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

## 9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our college may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

## 9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

## 9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------





- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## 10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 college days of receipt of a written request.

## 11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system to facilitate our cashless catering system where pupils use finger prints to receive college dinners instead of paying with cash we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The college will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the college's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can use PIN numbers to access the system to pay for college dinners if they wish.

Parents/carers and pupils can object to participation in the college's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the college's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object.

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------





Staff and other adults can also withdraw consent at any time, and the college will delete any relevant data already captured.

## 12. CCTV

We use CCTV in various locations around the college site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Principal.

## 13. Photographs and videos

As part of our college activities, we may take photographs and record images of individuals within our college. We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used. Uses may include:

- Within college on notice boards, college posters, prospectus and newsletters, etc.
- Outside of college by external agencies such as the college photographer, newspapers, campaigns
- Online on our college website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

## 14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the college's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------



- For the benefit of data subjects, making available the name and contact details of our college and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## 15. Data security and storage of records

We 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.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site it must be safeguarded, papers should be carried in locked briefcases. The use by staff of removable media eg USB sticks is not permitted.
- Passwords that are at least 8 characters long containing letters and numbers are used to access college computers, laptops and other electronic devices. Staff and pupils are automatically reminded to change their passwords at regular intervals
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for college-owned equipment (see our Online safety policy and Acceptable use agreements)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

## 16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the college's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## 17. Personal data breaches

The college will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the Data Breach Procedure attached to this Policy. When appropriate, we will report the data breach to the ICO within 72 hours. As example, breaches in a college context may include, but are not limited to:

- A non-anonymised dataset being published on the college website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a college laptop containing personal data about pupils

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------



## 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.

## 19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our college's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Proprietor and the Advisory Board.

## 20. Links with other policies

This data protection policy is linked to our:

- Online Safety Policy
- Acceptable Use of ICT Agreements
- Child Protection and Safeguarding Policies
- Security Policy

Produced by:	BB	Date:	05/05/18	Checked by:	MN	Date:	16/05/18	Approved by:	MW	Date :	18/05/18
--------------	----	-------	----------	-------------	----	-------	----------	--------------	----	--------	----------