LOCATION: SCHOOL HANDBOOK, SECTION 1, DOCUMENT 40

MEDWAY COUNCIL EDUCATION DEPARTMENT

DATA PROTECTION POLICY

(INCLUDING GENERAL DATA PROTECTION REGULATIONS AND PRIVACY NOTICES)

Date policy first adopted: October 2018
Date reviewed: November 2024
Reviewed By: Jo Dawson
Date ratified by Governing Body: November 2024
Date of next review: Autumn 2025

Contents

1. AIMS

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with the UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION & GUIDANCE

This policy meets the requirements of the: -

UK General Data Protection (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by the Data Protection, Privacy and Electronic Communications Amendments (EU Exit) Regulations 2020.

Data Protection Act 2018 (DPA 2018)

It also reflects the Information Commissioner's Office's (ICO) guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with Regulation 5 of the Education (Pupil Information) (England) Regulations 2006, which gives parents the right of access to their child's educational record.

3. DEFINITIONS

Term: Personal Data.

Definition: Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Term: Special categories of personal data.

Definition: Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation.

Term: Processing.

Definition: Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Term: Data subject.

Definition: The identified or identifiable individual whose personal data is held or processed.

Term: Data controller.

Definition: A person or organisation (school) that determines the purposes and the means of processing of personal data.

Term: Data processor.

Definition: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Term: Personal data breach.

Definition: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

Our school processes personal data relating to parents and carers, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES & RESPONSIBILITIES

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

5.1 Governing Body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

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.

They 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 school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO and, where applicable, Subject Access Requests.

The designated DPO at Abbey Court School is the Office Manager. Their contact details are below:

Contact Address: Abbey Court School, Cliffe Road, Strood, Kent ME2 3DL.
Contact Email: office@abbeycourt.medway.sch.uk
Contact Telephone: 01634 338220

5.3 HEADTEACHER

The Headteacher 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 school of any changes to their personal data, such as a change of address

• Contacting the DPO in the following circumstances:

a) With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.

b) If they are concerned that this policy is not being followed.

c) If they are unsure whether or not they have a lawful basis to use personal data in a particular way.

d) Whenever they are engaging in a new activity or project that may affect the privacy rights of the individual.

e) If there has been a data breach.

f) If they need support/guidance with any contracts sharing personal data with third parties or transferring personal data outside the UK.

g) If they need to rely on or capture consent, draft Privacy Notices deal with data protection rights invoked by an individual or transfer personal data outside the UK.

6. DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that our school 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 school aims to comply with these principles.

7. COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

• The data needs to be processed so that the school 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 school, 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 school (where processing is not for any tasks the school performs as a public authority) 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 under data protection law:

a) The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
b) The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law.
c) The data has already been made **manifestly public** by the individual
d) The data needs to be processed for the establishment, exercise or defence of **legal claims**
e) The data needs to be processed for reasons of **substantial public interest** as defined in legislation
f) The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
g) The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
h) The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.1 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.

We will keep data accurate and where necessary up to date. Inaccurate data will be rectified or erased where appropriate.

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 School's Toolkit 2019 (https://irms.org.uk).

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 contract with the supplier or contractor, 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.

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

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 internationally we will do so in accordance with UK 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 school 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.

• Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing

• The right to lodge a complaint with the ICO or another supervisory authority

• 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.

•The safeguards provided if the data is being transferred internationally.

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 and clearly dated.

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 concerning 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 below the age of 12 (Primary Schools) are generally not 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 school may 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.

Children aged 12 and above (Secondary Schools) 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 school 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 (or receipt of the additional information needed to confirm identity, where relevant.)

• 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.

• Would include another person's personal data that we can't reasonably anonymise and we do not have the other person's consent and it would be unreasonable to proceed without it.

•Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

A request will be deemed unfounded or excessive we may refuse to act on it, or charge a reasonable fee to cover administration costs. We will consider whether the request is repetitive in nature when making a decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access rights through the courts.

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.

• Ask us to rectify, erase or restrict the processing of their personal data.

• Prevent the use of their personal data for direct marketing.

• Object to processing that has been justified on the basis of public interest, official authority or legitimate interest.

• Challenge decisions based solely on automated decision-making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

• 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 days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

The right applies as long as the pupil concerned is aged 18 or under.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean realising exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 Data Protection Officer (DPO).

12. PHOTOGRAPHS & VIDEOS

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used by both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this Uses may include:

• Within school on notice boards and in school magazines, brochures, newsletters, etc.

• Outside of school by external agencies such as the school photographer, newspapers, and campaigns.

• Online on our school website or social media pages. We will monitor regularly websites, brochures and display boards to ensure that images of pupils are not used if they have left the school.

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.

Related school policy: See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this (Secondary age pupils only, or pupils where appropriate have agreed to this).

13. ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Abbey Court School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Abbey Court School will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 1.

14. DATA PROTECTION BY DESIGN & 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 data impact assessments where the school's processing of personal data presents a high risk to the 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:

a) For the benefit of data subjects, make available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).

b) For all personal data that we hold, maintaining an internal record of the type of data, the 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 & 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 secure when not in use.

• Where personal information needs to be taken off-site, staff must sign it in and out from the school office.

• Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.

• Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

• Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety policy on acceptable use).

• 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Data is stored and disposed of in line with the Information and Records Management Society's School's Toolkit 2019 (https://irms.org.uk).

17. PERSONAL DATA BREACHES

The school 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 procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

• A non-anonymised dataset being published on the school 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 school laptop containing non-encrypted personal data about pupils.

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 school's processes make it necessary.

19. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually by the full governing body.

20. LINKS WITH OTHER POLICIES

This data protection policy is linked to other policies including:

- Safeguarding / Child Protection Policy.
- E-Safety Policy.
- Staff ICT Code of Conduct and Acceptable Use Agreement.
- Use of Videos / photographs
- Data Retention

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

• On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO), by our reporting procedure, via email or telephone or in person.

• The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

a) Lost

b) Stolen

c) Destroyed

d) Altered

e) Disclosed or made available where it should not have been

f) Made available to unauthorised people

• Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

• If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors

• The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO where necessary, and the DPO should take external advice when required (e.g. from IT providers).

• The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

• The DPO will work out whether the breach must be reported to the ICO and individuals affected using the ICO's self-assessment tool.

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored In the school recording system.

Where the ICO must be notified, the DPO will do this via the Report a Breach Page on the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

a) A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.

b) The name and contact details of the DPO.

c) A description of the likely consequences of the personal data breach.

d) A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

• If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain why there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

a) A description in clear and plain language of the nature of the personal breach

b) The name and contact details of the DPO.

c) A description of the likely consequences of the personal data breach.

d) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, police, insurers, banks or credit card companies.

• The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

a) Facts and cause.

b) Effects.

c) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

• The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breaches, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

• If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

• Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

• If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department/external IT to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy as evidence if required).

• In any cases where the recall is unsuccessful, or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the

email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

• The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information be removed from their website and deleted.

• If safeguarding information is compromised the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all of its 3 safeguarding partners

Appendix 2 – School Privacy Notices

Abbey Court School

Privacy Notice - how we use pupil information

The categories of pupil information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results, post-16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)

This list is not exhaustive, nor limited to the above.

Why we collect and use pupil information

We collect and use pupil information, for the following purposes:

a) to support pupil learning
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us for DfE data collections
g) to comply with the law regarding data sharing

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing pupil information are: section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6 (1)(c) and Article 9 (2)(b) of the General Data Protection Regulation (GDPR).

How we collect pupil information

We collect pupil information via registration/data collection forms at the start of the school year or Common Transfer File (CTF) or secure file transfer from previous schools if applicable.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it is requested on a voluntary basis. To comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule. Data will be retained for all pupils enrolled at the school until the age of 31, after which they will be safely destroyed.

Who we share pupil information with

We routinely share pupil information with:

- schools/colleges that the pupils attend after leaving us
- our local authority (Medway)
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- NHS and health care professionals

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

Youth support services - Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our Local Authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child/pupil once they reach the age of 16 where applicable.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our Local Authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our Local Authority website.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and Local Authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of data collections, under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see the 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Vicky Aspin, Headteacher. The school will, on an annual basis, share individual Data Collection Sheets with you in order to ensure that records are accurate and up to date.

You also have the right to:

- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/.

Contact

If you would like to discuss anything in this privacy notice, please contact Vicky Aspin, Headteacher or the Data Protection Officer (the Office Manager).

How Government Uses Your Data

The pupil data that we lawfully share with the DfE through data collection:

- underpins school funding, which is calculated based on the number of children and their characteristics in each school.
- informs 'short-term' education policy monitoring and school accountability and intervention (for example, Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data-sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual-level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with the Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

To contact DfE: https://www.gov.uk/contact-dfe

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time.

This version was reviewed in November 2024.

Appendix 3 – Privacy Notice – how we use workforce information

Abbey Court School

Privacy Notice - how we use workforce information

The categories of school information that we process include:

- personal information (such as name, date of birth, employee or teacher number, national insurance number, address, telephone and e-mail contact details, car registration)
- special categories of data needed for the Disclosure and Barring Service and Single Central Register (such as DBS number, right to work in the UK, convictions/cautions)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, employee reference number, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information (such as health clearance information, and occupational health reports)
- other information to support the financial and personnel requirements of the school.

Why we collect and use workforce information

We collect and use staff information under the EU General Data Protection Regulation (GDPR).

We use workforce data to:

a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) to comply with the law regarding checks such as DBS and medical clearance
e) submit annual statistical returns to Central Government

Under the General Data Protection Regulation (GDPR), the legal basis/bases we rely on for processing personal information for general purposes are set out in Article 6 of the GDPR and Article 9 (Special Category Data). Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

Collecting workforce information

We collect personal information via PMC001 and Staff Data Collection forms. Workforce data is essential for the school's/Local Authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. Data will not be kept for longer than is necessary. The school follows the Information Commissioner's guidance on retention of documents, including the Information and Records Management Society's Retention Guidelines for School. See Information and Records Management Society's School's Toolkit 2019 (https://irms.org.uk).

Who we share workforce information with

We routinely share this information with:

- our Local Authority (where applicable)
- the Department for Education (DfE)
- another establishment when an employment reference has been requested

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so. Workforce data is shared with the Local Authority via the completion of Human Resource/Payroll forms to enable contracts to be created and staff to be paid on a regular basis. Workforce data is routinely collected by Central Government every Autumn by the school submitting a Workforce Census Return through the SIMS database to enable statistical analysis to be undertaken at a National level.

Local authority

We are required to share information about our workforce members with our Local Authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and Local Authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of data collection under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Vicky Aspin, Headteacher.

You also have the right to:

- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact Vicky Aspin, Headteacher.

How the Government uses your data

The workforce data that we lawfully share with the DfE through data collection:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required

- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time.

This version was reviewed in November 2024.

Appendix 4 - Information Sharing

Department for Education – Information Sharing – Advice for practitioners providing safeguarding services for children, young people, parents and carers.

May 2024

https://assets.publishing.service.gov.uk/media/66320b06c084007696fca731/Info_sharing_advice_content_May_2024.pdf