Cookridge Primary School
Data Protection Policy
2024- 2026

Adopted by governing body – September 2024

Review – when legislation is altered/updated or every 2 years

The Data Protection Policy will be published on the school website.

Contents

1. Aims

This Data Protection Policy outlines our commitment to maintaining the privacy and protection of personal data in accordance with the UK General Data Protection Regulation (GDPR) and relevant data protection legislation.

The policy is intended for:

- School Staff: All employees, including teaching and non-teaching staff, who handle personal data of students, parents, staff and other stakeholders
- School Leadership and Governors: Individuals responsible for overseeing and ensuring compliance with data protection practices
- Parents & Guardians: This policy provides essential information on how the school manages their children's personal data and outlines their rights regarding that data
- Third Party – Contractors: External organisations or individuals processing data on behalf of the school must understand their responsibilities under this policy.

We aim to make sure that all personal information about staff, students, parents, governors, visitors, and others is collected, stored, and used according to UK data protection laws (the UK General Data Protection Regulation and the Data Protection Act 2018). This policy covers all personal data, whether it is on paper or stored electronically.

2. Legislation and guidance

This policy meets our obligations under the:

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

Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's 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 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living 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.
Special categories of personal data	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
Processing	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.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data

	controller.
Personal data breach	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 handles personal data about parents, students, staff, governors, visitors, and others, which makes it a data controller. This is called processing within the legislation. The school is registered with the Information Commissioner's Office (ICO) and will pay the required registration fee each year or as legally needed.

5. Roles and 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 board

The governing board is responsible for ensuring the school meets all data protection requirements.

5.2 Data protection officer

The Data Protection Officer (DPO) is responsible for overseeing this policy, making sure we follow data protection laws, and creating related policies and guidelines as needed.

The DPO will submit an annual report on their work to the data protection lead in school who will share with the governing board and will also share any advice or recommendations on data protection issues when relevant.

The first point of contact for individuals whose data is processed by the school is the data protection lead. This is the school business manager/office manager/Headteacher. However, individuals may contact the DPO direct if the need arises. The DPO is first point of contact for the ICO.

Full details of the DPO's responsibilities are set out in the Service Level Agreement.

Our DPO is Richard Lewis-Ogden and is contactable via email at DPO@bywaterkent.co.uk

The school is registered with the ICO (Information Commissioner's Office) and has paid the required data protection fee.

5.3 Headteacher

The headteacher has overall operational responsibility for day-to-day data privacy and control matters.

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:
    - 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 UK
    - If there has been a data breach
    - 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

6. Data protection principles

The UK 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

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 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 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 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- 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
- 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
- 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

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

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.

7.2 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 their permission, 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 when appropriate.

In addition, 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 school's record retention schedule.

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 if this is appropriate 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 hire suppliers or contractors that can prove they follow UK data protection laws
    - Set up a data sharing agreement, either in the contract or as a separate document, if we are sharing significant or sensitive data, to ensure data is handled fairly and legally
    - Only share the data the supplier or contractor needs to provide their service and any necessary information to keep them safe

We will also share personal data with law enforcement or government bodies if legally required to do so.

In emergencies affecting our pupils or staff, we may share personal data with emergency services and local authorities to assist them in their response.

If we transfer personal data internationally, including to countries in the European Economic Area, we will follow UK data protection laws.

9. Subject access requests and other rights of individuals

9.1 Subject access requests(SARs - also called Data Subject Access Requests or DSARs)

Individuals have the right to request access to personal information that the school holds about them.

- This may include:
- Confirmation that their data is being used Access to a copy of their data
- The reasons for data processing
- The types of data being processed
- Who the data is shared with
- How long the data will be kept, or how this period is decided
- The right to request changes, deletion, restrictions, or to object to data processing
- The right to file a complaint with the ICO or other relevant authority
- The source of the data if not provided by the individual

- Whether automated decision-making affects their data and what impact it may have
- Any protections in place if their data is shared internationally

Subject access requests can be submitted in any format, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name/ Contact address/ Phone number and email
- Information being requested
- Reason for requesting the information (so that we locate and prioritise the datasets that will be of most value).

If staff receive a subject access request in any form, they must forward it to the data protection lead in school immediately.

9.2 Children and subject access requests

A child's personal data belongs to the child, not to their parents or carers. For a parent or carer to make a request for a child's data, the child must either not understand their data rights or have agreed to the request.

Generally, children under 12 are considered too young to fully understand these rights, so most requests from parents for pupils' data may be granted without the child's direct permission. However, this is assessed on a case-by-case basis

9.3 Responding to subject access requests

When we respond to requests:

- We may ask the individual for a form of ID.
- We may contact them by phone to confirm the request
- We will respond within 1 month of receiving the request or required identification
- We will provide the information at no cost
- If the request is complex, we may take up to 3 months and will inform the individual within 1 month, explaining the need for extra time

We may not provide information if it:

- Could seriously harm the physical or mental health of the student or another person
- Involves child abuse details where sharing would not be in the child's best interests
- Contains personal data about someone else that cannot be anonymised, and we do not have consent to share it
- Is part of certain sensitive documents like legal, crime, immigration, management, or exam-related records

If the request is unreasonable or repeated, we may refuse or charge a fee to cover costs. If we refuse a request, we will explain why and inform the individual of their right to contact the ICO or to seek a legal resolution.

The Data Protection Officer shall provide guidance and oversee the response ensuring that this is within the spirit of the principles of the UK GDPR and in accordance with the legislation.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request, individuals also have the right to:

- Withdraw their consent to data processing at any time
- Ask for correction, deletion, or limited processing of their data (in certain cases)
- Prevent their data from being used for direct marketing
- Object to data processing based on public interest or legitimate interests
- Challenge decisions made by automated data processing with no human involvement
- Be notified of a data breach (in some cases)
- Submit a complaint to the ICO
- Request that their data be transferred to another party in a structured, common, and machine-readable format (in certain cases)

Individuals can submit requests for these rights to the data protection lead or to the DPO. If staff receive such a request, they should forward it to the data protection lead who will consult the DPO.

10. Parental requests to see the educational record

Parents or those with parental responsibility have the legal right to access their child's educational record (which includes most information about the pupil) for free within 15 school days (term time) of submitting a written request.

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

This right applies as long as the pupil is under 18 years old.

In certain situations, this right may be denied, such as if sharing the information could cause serious harm to the physical or mental health of the pupil or another person, or if it would release exam marks before they are officially published

11. Biometric recognition systems and Artificial intelligence

11.1 Biometric recognition systems

Pupils

Under the Protection of Freedoms Act 2012, a "child" is defined as anyone under 18.
If we use pupils' biometric data in an automated recognition system (for example, if pupils use fingerprints to receive school meals instead of paying with cash), we will follow the rules of the Protection of Freedoms Act 2012.

Parents/carers will be informed before any biometric system is introduced or before their child uses it. The school will get written permission from at least one parent or carer before collecting and processing any biometric data from their child.

Parents/carers and pupils can choose not to use the school's biometric systems. We will provide alternative ways for pupils to access these services if needed.

By law, if a pupil does not want to use the biometric system or wants to stop using it, we will respect their choice and not process their data, even if we have consent from the parent or carer.

Staff
If staff members or other adults use the school's biometric systems, we will also get their permission before they start using it, and we will offer alternatives if they prefer not to participate. Staff and other adults can withdraw consent at any time, and the school will delete any related data already collected.

11.2 Artificial Intelligence (AI)

AI tools are now common and easy to use. Staff, students, and parents may be familiar with generative AI chatbots like ChatGPT and Copilot, the school understands that AI can help students learn, but it also has risks for personal and sensitive information.

To keep this information safe, no one is permitted to enter personal or sensitive data into unauthorised AI tools or chatbots. If anyone does enter such data into an unauthorised generative AI tool, the school will treat it as a data breach and will follow the procedures for handling personal data breaches outlined in Appendix 1.

12. CCTV

If we have CCTV installed, we may use CCTV in different areas around the school and grounds to help keep the site safe. We follow the ICO's guidelines on using CCTV and comply with data protection rules.

We don't need to get permission from individuals to use CCTV, but we make it clear where people are being recorded. Security cam eras are easy to see, and there are clear signs explaining that CCTV is in use.

If you have questions about the CCTV system, please contact the Headteacher

13. Photographs and videos

As part of our school activities, we may take photos and videos of people in our school.

We will get written permission from parents or guardians before taking photos or videos of their child for communication, marketing, and promotional use. We will clearly explain how the photos or videos will be used to both the parent or guardian and the student.

Any photos or videos taken by parents or guardians at school events for their own use are not covered by data protection laws. However, we will ask that those photos or videos, which include other students, are not shared publicly on social media for safety reasons, unless all relevant parents or guardians agree.

When the school takes photos and videos, they may be used in ways such as:

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

Parents or guardians can refuse their permission or change their mind at any time. If consent is withdrawn, we will delete the photo or video and take reasonable steps not to share it further.

When we use photos and videos in this way, we will not include any other personal information about the child to keep them anonymous.

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 school'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
- Putting appropriate checks in place if we transfer any personal data outside the UK where no adequacy agreements are in place
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making 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)
    - 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, or left anywhere else where there is general access
- Where personal information needs to be taken off site

- Where possible we will implement multi-factor authentication and strong passwords that are at least 10 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 and not reuse passwords from other sites
- 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.
- 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.

17. Personal data breaches

The school will do everything reasonable to prevent personal data breaches. If we suspect a data breach, we will follow the steps outlined in appendix 1. If we assess the breach to meet the threshold for reporting, we will report the breach to the Information Commissioner's Office (ICO) within 72 hours of finding out about it.

Examples of breaches in a school setting may include but are not limited to:

- A dataset that is not anonymous being posted on the school website,
- showing the exam results of students eligible for pupil premium
- Safeguarding information being shared with someone who is not allowed to see it
- The theft of a school laptop that has unencrypted personal data about students.

18. Training

All new staff are provided with data protection training as part of their induction process. In line with the ICO recommendation, refresher training will be provided to all staff regularly and not less than every 2 years , forming part of continuing professional development.

The governing board will take strategic responsibility to ensure that it has a good understanding of its duties and obligations.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every two years** in accordance with Department for Education's advice on statutory policies and will presented to the full governing board for approval.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of Information
- Staff code of conduct
- Acceptable use of ICT/Digital technology
- Safeguarding and Child Protection

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 lead person in the school/organisation, who will contact the DPO.

1. The DPO will assist in the investigation of the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

o Lost

o Stolen

o Destroyed

o Altered

o Disclosed or made available where it should not have been

o Made available to unauthorised people

2. The DPO will determine whether to alert the Head Teacher/Chair of Governors.

3. The DPO will assist in making all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

4. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

5. The DPO will determine whether the breach meets the threshold to be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms using the ICO's self-assessment tool.

6. The DPO will ensure that the decision is documented (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system, or on a designated software solution.

7. Where the ICO must be notified, the DPO will do this by telephone or via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

o 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

o The name and contact details of the DPO

o A description of the likely consequences of the personal data breach

o 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

8. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that 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

9. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact and ensure that any decision on whether to contact individuals is documented. If the risk is high, the DPO, or data protection lead will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out in plain language:

o The name and contact details of the DPO

o A description of the likely consequences of the personal data breach

o 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

10. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

11. The data protection lead person in School, with advice and/or support from the DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

o Facts and cause

o Effects

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

Records of all breaches will be stored on the school's computer system, or on a designated software solution.

• In the case of a significant breach, the DPO, headteacher or designated senior leader 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 breach, 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 data protection lead person as soon as they become aware of the error

• If the sender is unavailable or cannot recall the email for any reason, the data protection lead will ask the ICT department to recall it

• In any cases where the recall is unsuccessful, the data protection lead will 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.

• Written confirmation that the email has been deleted will be requested from all the individuals who received the data, confirming that they have complied with this request

- In the case of a serious breach, we will arrange for an internet search to be conducted 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 is removed from their website and deleted

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

Privacy Notice (How we use workforce information)

Workforce is defined as all paid staff including those on placements, secondments, and agency staff. It will also include local authority staff engaged and paid by the governors of the school and for unpaid staff /volunteers.

The categories of school information that we process

These include:

- personal information (such as name, employee or teacher number, national insurance number, date of birth and address including emergency contacts)
- medical and disability information
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles, and salary information for payroll)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)

This list is not exhaustive, to access the current list of categories of information we process please see the school's Data Map, sometimes called the Record of Processing Activity (RoPA).

Why we collect and use workforce information

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 HMRC and employment legislation

Under the UK General Data Protection Regulation (UK GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:

Article 6 (1) (c). processing is necessary for compliance with a legal obligation to which the controller is subject." and 6 (1) (e) - **processing is necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller"

In addition, concerning any special category data we rely on Article 9:

- Article 9 (2) (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
- 9 (2) (c) To protect the vital interests of the individual;
- 9 (2) (f) in the event of legal claims or judicial acts,
- 9 (2) (i) As required for purpose of public health (with a basis in law)

Collecting workforce information

We collect personal information from individuals directly, e.g., from application forms, starter paperwork, staff contract forms, data collection exercises and consent forms

Workforce data is essential for the school to function. 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 UK 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 and that you can change your mind at any time.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please see the Data Map/RoPA and the Information and Records Management (IRMS) Toolkit for Schools IRMS Schools Toolkit - Information and Records Management Society

Who we share workforce information with

We routinely share this information with:

- our Local Authority (LA) Children's Services, the LA payroll department,
- the Department for Education (DfE)
- HM Revenue and Customs (HMRC)
- HR (Human Resources) provider
- Occupational Health
- Insurance company

This list is not exhaustive.

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.

Local authority and Department for Education (DfE)

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.

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

All data is transferred securely and held by the Department for Education (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.

HM Revenues and Customs (HMRC)https://irms.org.uk/general/custom.asp?page=SchoolsToolkit

The HMRC collects information about employees to maintain tax records and National Insurance (NI) contributions data in accordance with employment law and a number of statutory regulations and instruments (NI, Statutory Sick Pay, Statutory Maternity Pay etc).

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 the Head Teacher or the Data Protection Officer.

You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e., permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

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/

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the school office.

Last updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2023

Contact

If you would like to discuss anything in this privacy notice, please contact: **Richard Lewis-Ogden, Data Protection Officer on DPO@bywaterkent.co.uk**

How Government uses your data

The workforce data that we lawfully share with the Department for Education (DfE) through data collections:

- informs the Department for Education (DfE) 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 (DfE) 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 for Education (DfE)

The Department for Education (DfE) 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 for Education (DfE) 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 the Department for Education (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.

How to find out what personal information the Department for Education (DfE) hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data

- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Privacy Notice (How we use information about pupils and their families (children, parents and carers)

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 pupil premium/ 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 2 and phonics results any relevant results)
- behavioural information (records of incidents and exclusions and any relevant alternative provision put in place)

This list is not exhaustive, to access the current list of categories of information we process please see the school's data processing map, also referred to as the Record of Processing Activities (RoPA).

Why we collect and use pupil information

We collect and use pupil information and that of their families, for the following purposes:

a) to support pupil learning, assessment and special educational needs, as appropriate
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 the Department for Education (DfE) data collections and health services.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing pupil information are:

Article 6 (1) (c). processing is necessary for compliance with a legal obligation to which the controller is subject." and 6 (1) (e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

In addition, concerning any special category data we rely on Article 9:

- Article 9 (2) (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
- 9 (2) (c) To protect the vital interests of the individual,
- 9 (2) (f) in the event of legal claims or judicial acts,
- 9 (2) (i) As required for purpose of public health (with a basis in law)

Storing pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule. We have adopted the Information and Records Management Society (IRMS) recommendations as our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please see the Data Protection Policy and the IRMS Toolkit for schools IRMS Schools Toolkit - Information and Records Management Society

Who we share pupil information with

We routinely share pupil information with (not exhaustive):

- schools that the pupils attend after leaving us
- our local authority
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- National Health Service
- Targeted and family support services
- The Police
- The Courts and the Children and Family Court Advisory and Support Service (Cafcass)

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. For example, we must share pupil information in accordance with the Education (Pupil Information) (England) Regulations 2005 and Keeping Children Safe in Education Statutory Guidance.

Department for Education (DfE)

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 those data collections, under: section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by the Department for Education (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, 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, please contact the Head Teacher in the first instance or alternatively contact the school's Data Protection Officer (DPO), Richard Lewis-Ogden via email to DPO@bywaterkent.co.uk

You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

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/

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the School Office

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated in August 2023.

Contact

If you would like to discuss anything in this privacy notice, please contact: Richard Lewis-Ogden, Data Protection Officer (email DPO@bywaterkent.co.uk)

How Government uses your data

The pupil data that we lawfully share with the Department for Education (DfE) through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or 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 (DfE) (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 (DfE) 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 for Education (DfE).

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 for Education (DfE)

The law allows the Department for Education (DfE) to share pupils' personal data with certain third parties, including:

- schools and 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 for Education's (DfE) 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 the Department for Education (DfE) to request access to individual level information relevant to detecting that crime.

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

How to find out what personal information the Department for Education (DfE) holds about you

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Privacy Notice for visitors to our school

Why are we giving this to you?

When you visit our school, we will ask for and collect data about you for safeguarding purposes. This document sets out what personal data we will collect when you visit. Anything that we do with your personal data is known as "processing."

This document explains why we process that data, who we share this information with, and your rights in relation to your personal data processed by us. We also explain below how the school keeps your information safe.

If you want to know anything about the information that we keep, contact details can be found at the end of this document.

Policy Statement

Visitors (including parents of children on roll) are asked to sign in at reception. Signing in involves giving some information and registering a photograph on the school visitor management system, **SignIn.** If your visit is planned as part of an educational activity we may ask you to complete a visitor form.

What information do we hold about you (and your child, if appropriate) and where do we get it from:

We will collect, hold, share and otherwise use information about you and your child as set out in the boxes below:

	Where do we get it from?	*Why we need it?*
Your name(s)	You	To issue visitor passes and for identification around school
Your image	SignIn and CCTV	To safeguard all students and staff both during and outside of school hours when they are on our site
Vehicle registration	You	To keep a log of the cars in our car park
Additionally – if your visit is part of an educational activity		

Organisation	You	To keep a log of the organisations we work with
DBS information	You	To safeguard our students
Your consent to the use of your image (or not)	You	To ensure we understand your wishes in relation to your image

We are required to process visitor data in order to comply with our public task, in accordance with Article 6.1.e of the Data Protection Act 2018 (DLA 2018) namely to ensure that the security of our pupils, staff, visitors, buildings and their contents are always maintained.

How long will we hold your information?

We will hold information relating to you only for as long as necessary. Visitor information is automatically deleted from our visitor management system after **6 years** in accordance with the recommendation of the Information and Records Management Society (IRMS).

Contact information such as email address may be stored for longer to maintain contact over time but you can request that your data is deleted at any time.

Who will we share your information with?

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

Keeping this information safe

It is very important that only people who need to use your information can see it. The school keeps your information safe by putting in place procedures and technologies to make sure all information about you and your child is safe, from when we collect it to when we destroy it.

Security procedures include:

- Entry controls for the site and buildings. All staff wear photo-ID on school lanyards. All authorised DBS-checked visitors wear photo-ID on green school lanyards. Visitors/contractors wear photo-ID on red lanyards. Our door locks are programmed to only respond to codes which are available only to staff.

- Secure lockable desks and cupboards etc.

- Equipment. Staff are trained to ensure that individual PC monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

- Training. We provide training to our staff and pupils on the importance of keeping data secure

Your rights in relation to your information

You can ask to see the information we hold about you. If you wish to do this you should contact the headteachers PA in the first instance. (Contact details are on the school website)

You also have the right to:

- Object to what we are doing with your information (but remember that some of the things that we do have to be done by law)
- Have inaccurate or incomplete information about you amended
- Ask us to stop doing certain things with your information in some cases
- Make a claim against the school in certain circumstances where you have suffered as a result of the school breaching your data protection rights

If you feel it necessary to do any of the above, you can speak with the headteacher's PA who will arrange a meeting with you. The school does not have to meet all of your requests but we will let you know where we are unable to do so.

Concerns

If you are concerned about how we are using your personal data you should contact the Head Teacher. Alternatively, and if the matter is not resolved in school, you can contact our Data Protection Officer: Richard Lewis-Ogden at DPO@bywaterkent.co.uk

If there are still concerns, you can contact the Information Commissioner's Office should you consider this to be necessary, at https://ico.org.uk/concerns/.

Privacy Notice for Job Applicants

The school is registered with the information Commissioners Office (ICO) under the provisions of the UK General Data Protection Regulation (GDPR) and Data Protection Act. The school takes its responsibilities under the GDPR very seriously. This notice provides details of how we collect and uses information about you.

What is this information?

We may collect some or all of the following information about you as part of our recruitment process:

- Name, address and contact details
- Application data and application history
- Education and employment details
- Gender, ethnicity, disability, sexual orientation and religion/belief
- Date of birth and national insurance number, Identification, Immigration and Asylum details, i.e. right to work in the UK
- References if you are invited to interview
- Right to work in the UK and supporting documentation if you are invited to interview
- Copies of qualifications if you are invited to interview

Who uses this information?

People involved in the recruitment process for example, School Business Manager, Headteacher and Governors.

What authority do we have to collect and use this information?

Under the GDPR we collect and use this information under powers given to schools for the legitimate interests of the controller or third party, where applicable.

The following categories of lawfulness apply:

- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

In rare circumstances where no legal authority exists to use your information, we will obtain your express consent first.

What is 'personally identifiable data' (PII)?

The term PII relates to any data that could potentially identify a living person. The following fields in Human Resources are classified as PII: name, age, address, place of birth, date of birth, gender, national insurance number, any application data and any information about an individual that can be used directly, or in connection with other data, to identify, contact or locate that person.

Why do we use this information?

We use this information in the course of recruiting members of staff.

Who are we likely to share this information with?

We may sometimes share the information we have collected about you where it is necessary, lawful and fair to do so. In each case we will only share the minimum amount of information, only when required, for the following reasons:

With the local authority and our HR services provider to allow managers to manage recruitment processes.

How do we keep this information secure?

Your information is stored securely on database and document management systems with stringent limited access. All access to documents is limited to only those staff involved within the recruitment process.

How long do we keep this information?

Documents are kept for a period of 6 months following the end of the recruitment process. If you are successfully appointed into a post, your data will be held in line with school policies. A copy of the staff privacy notice will be provided to you upon appointment with full details.

What are your rights?

You have the right to request that we stop processing your personal data. Wherever possible, we will seek to comply with your request but we may need to hold or process information in connection with one or more of the school's legal functions.

If you have any questions about our use of this data, or you wish to request a copy of the information we hold about you, or you wish to discuss your rights in relation to opting out from these processes, please contact our **Data Protection Officer, Richard Lewis-Ogden** who can be contacted by email at dataprotection@carrmanor.org.uk .