
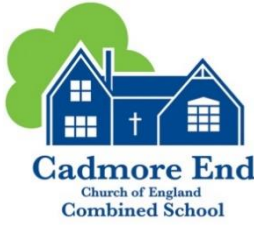


Data Protection Policy

The Oxford Diocesan School Trust	Cadmore End CofE School
	
Data Protection Policy	

Date implemented : May 2018

Last reviewed: January 2025

Member of staff responsible: Headteacher



Data Protection Policy

Contents

1. Aims	3
2. Legislation & Guidance	3
3. Definitions.....	3
4. The Data Controller	4
5. Roles & Responsibilities	5
6. Data Protection Principles.....	6
7. Collecting Personal Data	6
8. Sharing Personal Data.....	7
9. Subject Access Requests and other Rights of Individuals.....	8
10. Parental requests to see Educational Record	10
11. Biometric Recognition Systems	10
12. CCTV.....	10
13. Photographs & Videos	11
14. Data Protection by Design & Default.....	11
15. Data Security & Storage of Records	12
16. Disposal of Records.....	12
17. Personal Data Breaches	13
18. Training	13
19. Monitoring Arrangements.....	13
20. Links with Other Policies.....	13
21. Contact Us.....	13
Appendix 1 – Personal Data Breach Procedure.....	15
Appendix 2 – Model Privacy Notice for Pupils.....	18
Appendix 3 – Model Privacy Notice for Workforce	25

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation & Guidance

This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It is based on current guidance published by the Information Commissioner’s Office (ICO), including its code of practice for subject access requests and surveillance systems where applicable. If the School uses CCTV: It also reflects the ICO’s code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child’s educational record.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal Data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual’s:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.</p>

Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • 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	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
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 processes personal data relating to parents, pupils, staff, governors, 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.

Governing board

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

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board 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.

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

Our DPO service is provided by Little Chalfont Primary School and our Data Protection Officer (DPO) is Rob Hacking. He can be contacted at:

rhacking@littlechalfont.bucks.sch.uk or:

Little Chalfont Primary School,
Oakington Avenue,
Little Chalfont,
Buckinghamshire,
HP6 6SX

Staff, parents, and data subjects may contact the DPO for any queries relating to data protection rights or concerns..

Headteacher and SLT

The headteacher and SLT also acts as the representative of the data controller on a day-to-day basis.

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 European Economic Area
- 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 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

a. Lawfulness, fairness and transparency

We will only process personal data where we have one of six lawful bases under UK GDPR. The basis for processing depends on the type of data and its purpose:

- **Public interest task:** Processing required for providing education and safeguarding (e.g., attendance records, safeguarding reports).
- **Legal obligation:** Compliance with laws such as school census reporting.
- **Vital interests:** Protection of life, such as in medical emergencies.
- **Contract:** Processing necessary for employment or service agreements (e.g., payroll, staff contracts).
- **Legitimate interest:** Processing required for school operations where individual rights do not override (e.g., security monitoring).
- **Consent:** Used when no other legal basis applies (e.g., marketing, photo permissions)."

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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

b. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. Sharing Personal Data

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

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

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations

- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests and other Rights of Individuals

a. 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
- 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

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

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

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

b. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 (Primary School):

Children under 12 are generally presumed not to have sufficient understanding to make a Subject Access Request (SAR). Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil.

However, we assess each request on a case-by-case basis, considering:

- The child's maturity and understanding of their rights.

- The nature of the personal data being requested.
- Whether responding to the request would be in the child's best interests.

Parents or carers may submit requests on behalf of children, but where a child is deemed competent, their consent will be required before responding.

Children aged 12 and above (Secondary School):

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our 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.

c. Responding to subject access requests

When responding to requests, we:

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

We will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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

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

10. Parental requests to see Educational Record

The ODST policy for academies is that whilst not legally required, in a similar way to maintained schools, we give the right for parental access to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. Biometric Recognition Systems

The school does not currently use biometric data. If introduced in the future, written consent from at least one parent or carer will be required, and alternative authentication methods will be provided.

12. CCTV

The School may use CCTV in various locations around the school site to ensure it remains safe. If we use CCTV we will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Data Protection Officer (DPO)

13. Photographs & Videos

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

Pupils aged under 18 years of age

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 to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within 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

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.

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

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 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
- 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 & Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- All school accounts and devices must be secured using strong passwords (minimum 8 characters, including letters, numbers, and symbols). Multi-factor authentication (MFA) should be enabled where available... 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 where personal information is stored
- 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.

When using third-party disposal services, we will:

- Ensure the provider complies with UK GDPR.
- Obtain a Certificate of Secure Disposal.
- Verify that electronic records are permanently erased (not just deleted).

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 biennially or sooner if required due to significant changes in data protection law, ICO guidance, or school practices. The governing board will approve any material amendments.

20. Links with Other Policies

This data protection policy is linked to other policies including:

- Freedom of information policy (Including publication scheme)

21. Contact Us

Our DPO's contact details are below:

Rob Hacking
rhacking@littlechalfont.bucks.sch.uk
Little Chalfont Primary School,
Oakington Avenue,
Little Chalfont,
Buckinghamshire,
HP6 6SX

Telephone: 01494 762109

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 DPO
- 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:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- 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, 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)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must 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, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (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 by the DPO

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours.

As required, the DPO will set out:

- 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
- The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to contain 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - 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 notify any relevant third parties who can help mitigate the loss to individuals – for example, the 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:
 - Facts and cause
 - Effects
 - 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 by the DPO on the Trust's central systems.

- 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 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 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 to recall it
- In any cases where the recall is unsuccessful, the DPO 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
- The DPO will ensure we receive 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 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

Appendix 2 – Model Privacy Notice for Pupils

Y

Cadmore End School Data Retention Policy

1. Introduction Cadmore End School is committed to compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines the retention periods for pupil, staff, and financial records to ensure data is stored securely and disposed of appropriately.

2. Pupil Records

Record Type	Retention Period	Action After Expiry
Pupil Education Records	Until pupil leaves, then transferred to the next school	Secure transfer to new school
Attendance Registers	3 years after the end of the school year	Securely destroyed
Special Educational Needs (SEN) Records	31 years if an EHCP is in place, otherwise 6 years after pupil leaves	Securely destroyed
Child Protection/Safeguarding Records	Until the child turns 25	Securely destroyed unless required for legal proceedings
Medical and Accident Records	25 years from the date of the incident	Securely destroyed
Parental Contact Information	Deleted/anonymised after child leaves unless legally required	Secure deletion

3. Staff Records

Record Type	Retention Period	Action After Expiry
Personnel Files (including contracts and employment history)	6 years after employment ends	Securely destroyed
Payroll and Salary Records	7 years	Securely destroyed
DBS Checks	6 months after recruitment decision	Retain only reference that check was completed
Staff Absence and Sickness Records	3 years after tax year	Securely destroyed
Pension Records	12 years after benefit ceases	Securely destroyed

4. Financial Records

Record Type	Retention Period	Action After Expiry
Annual Accounts	6 years	Securely destroyed

Invoices and Receipts	6 years	Securely destroyed
Payroll and Tax Records	7 years	Securely destroyed
School Fund Records	6 years	Securely destroyed

5. Secure Storage and Disposal All records must be stored securely in locked filing cabinets or password-protected digital systems. When retention periods expire, documents should be securely shredded or permanently deleted.

6. Review and Compliance This policy will be reviewed annually to ensure compliance with current regulations. Any changes will be communicated to relevant staff.

Approved by: Headteacher / Data Protection Officer

Date: [Insert Date]

Appendix 3 – Model Privacy Notice for Workforce

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school. We, the school, are the 'data controller' for the purposes of data protection law. Our data protection officer is listed below (see 'Contact us' below).

The categories of school information that we process

These include:

- personal information (such as name, employee or teacher number, national insurance number, addresses, payroll information)
- characteristics information (such as, sex, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- 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 [\[link to website or location of data asset register / current privacy notice\]](#)

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

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

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- a) processing is necessary for compliance with a legal obligation to which the controller is subject;
- b) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- c) 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;
- d) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Processing of personal data revealing racial or ethnic origin, religious or philosophical beliefs, data concerning health shall be prohibited unless;

- a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- a) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- b) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- c) processing relates to personal data which are manifestly made public by the data subject;
- d) processing is necessary for reasons of substantial public interest, on the basis of [F4domestic law] which shall be proportionate to the aim pursued F5... and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

Collecting workforce information

We collect personal information via **[explain method of data collection used, for example, staff contract 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 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.

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 visit [16 Disposal of Records](#)

Who we share workforce information with

We routinely share this information with:

- our local authority (where applicable)
- the Department for Education (DfE)

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.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals

- The Department for Education
- Your family or representatives
- Educators and examining bodies
- Our regulator, Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations •
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

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 (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 children and young people with the Department for Education (DfE) for the purpose of those data collections, under: section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

We are required to share information about our school employees with the Department for Education (DfE) 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 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.

For privacy information on the data the Department for Education (DfE) collects and uses, please see: <https://www.gov.uk/government/publications/privacy-information-education-providers-workforce-including-teachers>.

Requesting access to your personal data

The UK-GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact our DPO (see 'Contact us' below)

You also have the following rights:

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request, data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to [complain to the Information Commissioner](#) if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

If you have a concern 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 [raise a concern with ICO](#)

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 our DPO (see 'Contact us' below)

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 on January 2025

Contact us

If you would like to discuss anything in this privacy notice, please contact our DPO, whose details are below:

Rob Hacking
rhacking@littlechalfont.bucks.sch.uk
Little Chalfont Primary School,
Oakington Avenue,
Little Chalfont,
Buckinghamshire,
HP6 6SX

Telephone: 01494 762109

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) will only share your personal data where it is lawful, secure and ethical to do so and 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 public benefit, proportionality, legal underpinning and strict information security standards.

For more information about the Department for Education's (DfE) data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the Department for Education (DfE) has provided information, (and for which project) 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) hold about you

Under the terms of UK GDPR, 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>

or

<https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights>

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