



Privacy Notice for Employees

Under data protection legislation, 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 when we process their personal data. This privacy notice explains how and why we collect, store and use personal data about Employees under the following legislation:

- UK General Data Protection Legislation (UK GDPR)
- Data Protection Act 2018 (DPA)
- The Data Use and Access Act 2025 (DUAA).

We, Cippenham Nursery School, are the 'Data Controller' for the purposes of data protection law. The School is registered as a Data Controller with the Information Commission (ICO). Our registration number is **Z8629609**.

Our data protection officer is The Schools People (see 'Contact us,' below).

1. Data Protection Principles

Personal Data must be processed in line with the six Data Protection Principles. It must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Privacy Notice for Employees

2. Types of Personal Data Processed by the School

The categories of employee information that we collect, create, hold, and share include, but are not limited to:

- personal information (such as name, address, telephone number, email address, employee or teacher number, national insurance number, and bank account number)
- pre-employment and safeguarding checks such as “Right to Work in the UK” information, DBS and Children’s Barred List outcome information, pre-placement medical questionnaire outcome information, employment references, overseas check outcome information, and Teacher Status Check outcome information
- contract information such as start dates, hours worked, post, roles, salary information, and continuous service dates
- work absence information, such as number and type of absences and reasons, and occupational health medical referrals and reports
- performance management, grievance, and conduct or disciplinary information [where applicable]
- settlement agreements, COT3 agreements, and claims to an Employment Tribunal or Employment Appeal Tribunal [where applicable]
- qualifications and, where relevant, subjects taught
- employee benefit information
- payroll information: Salary and salary history, benefits, tax, NI and NI number, tax status, pension contributions, other deductions, student loans, timesheets, CCI’s etc.
- pension information
- details of driving licence, passport and other relevant identity documents
- any other personal data we will inform you of from time to time

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity, and religious affiliation
- Trade union membership
- Information about your health, including any medical condition, health and sickness records
- Information you make public, such as on social media, where this is brought to our attention and we have concerns regarding the content

Privacy Notice for Employees

- Information about your criminal record (see section 5 below)
- Any other special category data we will inform you of from time to time

3. Collecting Personal Data

We collect employee personal data:

- From CVs and job application forms, and the recruitment process, either directly from individuals or indirectly via employment agencies
- From third parties, including references from previous employers, the Local Authority, or other agencies, your colleagues, parents and pupils
- From health providers such as your GP, Occupational Health and Fitness to Work notifications
- During your employment, including attendance records, sickness records, performance reviews and complaint/disciplinary/grievance investigations
- In addition, the school also uses CCTV cameras in and around the school site for security purposes and for the protection of staff, pupils and other stakeholders.

While the majority of employee information provided to us is mandatory, some is provided voluntarily. Whenever we seek to collect information relating to employees, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

If you fail to provide certain information when requested, we may be prevented from complying with our official or legal obligations (e.g. such as discharging our obligations to HMRC)

4. Why We Collect and Use Employee Information

We use employee data as part of our day-to-day business management and to manage our relationship with you in various situations during your recruitment, employment (or engagement) and even following the termination of your employment (or engagement). For example, to:

- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace

Privacy Notice for Employees

- operate and keep a record of employee performance and related processes, to plan for career development, succession planning and workforce management purposes
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- obtain occupational health advice, to comply with duties concerning individuals with disabilities, to meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the school complies with duties concerning leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration
- inform our recruitment and retention policies
- allow better financial modelling and planning
- provide references on request for current or former employees
- enable equality monitoring
- respond to and defend against legal claims

Where appropriate, we will seek consent to process personal data when no other lawful basis for processing exists. For example, to use your personal data for marketing purposes. Employees may withdraw the consent given in these circumstances at any time.

5. Automated Decision Making

Automated decision-making takes place when an electronic system uses personal information to make decisions without human intervention. We are permitted to use automated decision-making in limited circumstances.

The School does not currently carry out any automated decision-making or profiling. If this position changes, we will notify you and implement appropriate safeguards, as required by law.

Privacy Notice for Employees

6. The Lawful Bases on which we Process Personal Data

We only collect and use personal data when the law and our policies allow us to do so. We process general category data where:

- the data subject, or a person with the lawful authority to exercise consent on the data subject's behalf, has given explicit consent
- the processing is necessary for a contract we have with you, or because we have asked you to take specific steps before entering into a contract
- the processing is necessary for us to comply with the law
- the processing is necessary to protect your vital interest or that of another person
- the processing is necessary for us to perform a task in the public interest or for our official functions, and this task or function is lawful
- the processing is necessary for our legitimate interest, where the school is not acting in its official capacity.

As a public authority, the School primarily relies on public task and legal obligation as its lawful bases.

In addition, the DUAA 2025 introduces the concept of recognised legitimate interests. In limited circumstances, the Trust may rely on legitimate interests without completing a full Legitimate Interests Assessment when the processing falls within categories recognised under the Act. This does not replace our reliance on the "public task" basis for our core educational functions.

We process 'special category' data where :

- the data subject, or a person with the lawful authority to exercise consent on the data subject's behalf, has given explicit consent
- necessary to carry out our obligations relating to employment law
- necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent
- the processing relates to personal data which are manifestly made public by the data subject;
- necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- necessary for reasons of substantial public interest,

Privacy Notice for Employees

- necessary, where applicable, for preventative or occupational medicine to assess the working capacity of the employee or to obtain a medical diagnosis
- necessary for the purposes of public health
- necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Some of the reasons listed above for collecting and using personal data overlap, and there may be several grounds which justify our use of this data.

7. Criminal Proceedings/Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations, provided we do so in line with data protection legislation.

We envisage that we will hold information about criminal convictions, for example, if it comes to light as a result of our appointment and Disclosure and Barring Service checks, or during your time as an employee.

Where appropriate, such information may be shared with external agencies, including the child protection team at the Local Authority, the Local Authority Designated Officer, and/or the Police.

Such information will be processed only to the extent permitted by law, and appropriate measures will be taken to keep the data secure.

8. Consent

We may process your personal information without your consent, in compliance with the above lawful bases, where this is required or permitted by law and our policies.

We will seek consent to process personal data where no other lawful basis exists. For example, if we wish to use your photographs for marketing purposes.

In limited circumstances, we may approach you for your written consent to allow us to process 'special category' data (e.g. to obtain an occupational health report). If we do so, we will provide you with full

Privacy Notice for Employees

details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

Where we rely solely on your consent as the lawful basis for processing, you have the right to withdraw consent in writing at any time.

9. Change of Purpose

We will only use employee personal data for the purposes for which it was collected, as set out in this privacy notice, unless we reasonably consider that we need to use it for another purpose and that purpose is compatible with the original purpose.

Examples of compatible further use can include processing related to safeguarding, workforce management, payroll and pensions administration, compliance with legal obligations, internal and external audit, equalities monitoring, and the establishment, exercise or defence of legal claims.

If we need to use your personal information for a purpose incompatible with the purpose for which it was collected, we will notify you before we begin the new processing. We will explain what we intend to do and the lawful basis we rely on, and, where required, we will seek your consent.

10. Storage and Retention of Personal Data

A significant amount of personal data is stored electronically. Some information may also be stored as a hard copy.

All data is stored and accessed following the School's **Data Protection Policy**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for including, to satisfy any legal, accounting, insurance or reporting requirements. Details of retention periods for different aspects of your personal information are available in our **Data Retention Policy**.

When your employment at the School ends, we will retain your personal information and securely destroy it in accordance with our **Data Retention Policy**.

Privacy Notice for Employees

11. CCTV

We have installed CCTV systems on our premises for the safety of staff, pupils, governors and other stakeholders, and for the prevention and detection of crime. Signs are displayed notifying you that CCTV is in operation.

All CCTV images will be retained for 25 days. After this period, the images are permanently deleted unless they are required for an identified ongoing incident/investigation (for example, if a crime has been observed and recorded or if the images have been retained while a subject access request is being processed. In such cases, images will be retained until the conclusion of the relevant process.

For further information, please refer to the School's **CCTV Policy**

12. Sharing Information

We do not share employee information with anyone without consent, unless required by law or permitted by our policies.

We routinely share employee personal data with:

- The Local Authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- The Department for Education - to fulfil our statutory reporting requirements. We are required to share information about our workforce with the 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 DfE under a combination of software and hardware controls that meet the current [government security policy framework](#). For more information, please see the 'How Government uses your data' section below.

We may occasionally share employees' personal data with:

Privacy Notice for Employees

- Governors
- Disclosure & Barring Service
- Ofsted
- Teaching Regulation Agency
- Teachers' Pension Service
- Local Government Pension Scheme
- The Police or other law enforcement agencies
- The Courts, if ordered to do so
- Prevent teams under the Prevent Duty on Schools
- Trade Unions and Associations
- Your family or representatives
- Our auditors
- Survey & research organisations
- Health Authorities
- Professional bodies

Other third-party service providers

We also share limited personal data with third-party service providers who require access to data to perform contracted services. These service providers include:

- Schools HR - our HR Provider
- Medigold - our Occupational Health provider
- Slough Borough Council Payroll Department to ensure you receive your contractual benefits
- Capita SIMS to facilitate database administration and technical support
- Cybersupport - IT support
- Our legal advisors and other consultants
- Our insurance providers
- Other third-party providers we will notify you about from time to time.

These third-party service providers act as data processors on the School's behalf and are required to take appropriate security measures to protect your personal information in line with our policies and data protection legislation. We authorise these service providers to use personal data only as necessary to perform services on our behalf, or to comply with legal obligations.

Privacy Notice for Employees

13. Transferring Data Outside the UK

We do not routinely transfer personal data outside the UK. Where international processing is necessary, we transfer personal data only in compliance with UK data protection law and only where appropriate safeguards are in place.

These safeguards may include:

- an adequacy decision under the UK GDPR; or
- approved contractual safeguards, such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses; and
- a completed Transfer Risk Assessment (TRA).

In exceptional circumstances, where no adequacy decision or appropriate safeguards apply, we may rely on a limited UK GDPR derogation (for example, where the transfer is necessary for important reasons of public interest or to protect vital interests).

14. Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Access to employee information is strictly controlled and aligns with the DUAA 2025 requirement to ensure that only staff with a legitimate and proportionate business need can access specific categories of data.

In addition, we limit access to your personal information to those agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have procedures in place to address any suspected data security breach and will notify you and any applicable regulator if required by law, in accordance with our **Data Security Policy and Breach Procedure**.

15. Your Data Subject Rights

You have the right to:

- Make a Subject Access Request (SAR) (see below)

Privacy Notice for Employees

- Withdraw your consent to processing at any time (in certain circumstances)
- Ask us to rectify, erase or restrict the processing of your personal data, or object to the processing of it (in certain circumstances)
- Prevent the use of your personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of the agreements under which your personal data is transferred outside of the UK
- Object to decisions based solely on automated decision-making or profiling. Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Raise a data protection complaint with the school
- Raise a complaint with 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).

For more information about your data subject rights, please see [here](#).

Your Duty to Inform us of Changes

It is important that the personal information we hold about you is accurate and up to date. Please keep us informed if your personal information changes during their time with us.

Subject Access Requests

Under data protection legislation, individuals have the right to request access to their personal data held by the School. Subject Access Requests **may be** made to the School in written form or verbally.

If you would like to make a SAR concerning your own personal data it would be helpful if this could be made in writing to the Headteacher, including your:

- name and contact address
- email address and telephone number
- details of the information required.

Privacy Notice for Employees

Clarification and "Stopping the Clock"

Where a Subject Access Request is unclear or requires further detail, the School may request clarification from the requester. During this clarification period, the statutory time limit for responding will be paused ("stopped") until the required information is received.

For more information about making a SAR please see [Getting copies of your information \(SAR\) | ICO](#)

Reasonable and Proportionate Searches

When responding to Subject Access Requests, the School will conduct reasonable and proportionate searches in accordance with the standards set out in the Data Use and Access Act 2025. Under this proportionality requirement, the School is not obliged to provide copies of information that the requester already possesses or can already access. The School will, however, acknowledge that such information is held and explain why it is not being re issued.

A helpful '**Guide to Making A Subject Access Request**' is available from the School office or as a download from the School website. It **is not** mandatory to make a Subject Access Request using the form. It will, however, assist you in structuring your SAR to provide the information we need to action your request without delay.

Fulfilling A Subject Access Request

The statutory time limit for responding to a Subject Access Request is one calendar month. This period begins once the School has received sufficient information to verify identity and clarify the scope of the request. Where clarification or identification is required, the response deadline may be paused until this information is provided.

A SAR is considered 'valid' only when we are fully satisfied with the requester's identity and their entitlement to the requested data. If in any doubt, we will request confirmation of identity to ensure your personal data is not inadvertently released to a third party who is not entitled to it.

Given that the School has limited staff resources outside term time, we encourage employees to submit Subject Access Requests during term time and to avoid sending requests during periods when the School is closed or about to close for the holidays. This will help us respond to your request as promptly as possible.

Privacy Notice for Employees

If the SAR is complex or numerous, the period in which we must respond may be extended by a further two months. You will be notified of any delays in actioning the SAR and provided with a timeframe in which you can expect to receive the requested data.

Fees

You will **not** have to pay a fee to access your personal information (or to exercise any of your other data subject rights). However, we may charge a reasonable fee if your access request is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

For further information about how we handle Subject Access Requests, please see our ***Subject Access Request Policy and Procedure***

Exercising Other Data Subject Rights

If you wish to review, verify, correct or request the erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the school in the first instance (details below).

The Right to Withdraw Consent

Where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, and there is no other applicable lawful basis for processing the data, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Headteacher (details below).

Once we receive notification that you have withdrawn your consent, we will no longer process your information for the purpose (s) you originally agreed to, unless we have another lawful basis to do so.

16. Data Protection Complaints

Under the Data Use and Access Act 2025, employees' now have a new statutory right to complain directly to the School if they believe their data protection rights have been infringed. The School takes data protection concerns seriously and is committed to resolving complaints fairly, promptly and transparently. This new right gives the school the opportunity to investigate concerns and provide a

Privacy Notice for Employees

meaningful response before escalation.

If you have a concern about how we collect, use or protect your personal data, you should contact us using the details in the 'Contact' section of this notice, clearly explaining:

- the nature of your concern; and,
- the outcome you are seeking.

We will acknowledge and respond to complaints in line with statutory requirements and applicable timescales.

If you remain dissatisfied after receiving our final response, you have the right to escalate your complaint to the Information Commission (ICO). Further information about making a data-protection complaint is available on the ICO's website: [Make a complaint | ICO](#)

17. Contact Details

Data Controller: Cippenham Nursery School, St Andrew Way, Slough SL1 5NL

Data Controller's Representative: Nisha Gill, Headteacher. Email:

head@cns.slough.sch.uk

Data Protection Officer (DPO): The Schools People Email: dposervice@schoolspeople.co.uk

18. Changes to this Privacy Notice

This Privacy Notice will be reviewed every year or as necessary in response to changes in Data Protection legislation or our processing activities.

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new Privacy Notice when we make any substantial updates.

Effective Date: May 2018

Last update: April 2026

Review Date: April 2027

How the Government uses your data

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

Privacy Notice for Employees

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

Data collection requirements

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

Sharing by the Department

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

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

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

- who is requesting the data?
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

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

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data

Privacy Notice for Employees

- 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, you should make a 'subject access request'. Further information on how to do this can be found within the Department's 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: <https://www.gov.uk/contact-dfe>