



Privacy Notice for Job Applicants

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 where we are processing their personal data. This privacy notice explains how and why we collect, store and use personal data about Job Applicants

This privacy notice explains how and why we collect, store and use personal data about Job applicants 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 Commissioner's Office (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 following 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.

2. Types of Job Applicant Information We Collect.

The categories of Job Applicant information that we may collect, process, hold, and share include, but are not limited to:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- medical details, N.I. number;
- information about your entitlement to work in the UK
- assessment and opinion relating to the recruitment process

We may also collect, store and use information about you that falls into “special categories” of more sensitive personal data. This may include information about (where applicable):

- Race, ethnicity, religious or philosophical beliefs, sexual orientation
- Disability, health, and access requirements

3. Collecting Personal Data

We collect Job Applicant personal data from:

- Application forms and CVs
- From documents provided to prove your identity and entitlement to work in the UK such as passports or other identity documents
- During the interview process and other forms of assessment therein,
- From third parties such as references from current/former employers and others
- DBS checks
- Occupational health such as pre-employment health checks
- CCTV cameras in and around the school site

In addition, we may conduct an online search as part of our due diligence on the shortlisted candidates to identify any publicly available issues we may wish to explore at the interview.

We do this in line with the guidance in section 226 of Keeping Children Safe in Education (2024). Any search conducted will be proportionate to assessing the candidate’s suitability to work in a regulated activity and with appropriate safeguards.

4. Why we Collect and Process Job Applicant Information

The purpose of processing Job Applicant personal data is to support the school in:

- Making decisions on whether to appoint you
- Checking your suitability to be an employee of the School
- Facilitating safe recruitment, as part of our safeguarding obligations towards pupils
- Identifying you and safely evacuating the School in the event of an emergency
- Enabling equalities monitoring
- Ensuring that appropriate access arrangements can be provided for job applicants who require them
- Sending you communications relating to your job application
- Complying with health and safety obligations
- Maintaining and promoting equality
- Monitoring recruitment statistics
- Receiving advice from external advisors and consultants
- Responding to and defending legal claims

While the majority of information we collect about job applicants is mandatory, there is some information that may be provided voluntarily.

Whenever we collect information about job applicants, 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 unable to comply with our recruitment process and legal obligations.

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.

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 as provided consent for one or more specified purposes
- necessary for the performance of a contract, or to take steps prior to entering into a contract with you
- necessary to comply with a legal obligation
- necessary to protect the vital interests of the data subject or another person
- necessary to perform a task in the public interest or for our official functions
- necessary for our legitimate interest, where we are not acting in our official capacity as a Nursery School

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:

- we have obtained explicit consent from the data subject
- 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
- necessary, for the purposes of preventative or occupational medicine to assess the working capacity of the employee or to obtain a medical diagnosis

- 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. Consent

We may process personal information in compliance with the above lawful bases where required or permitted by law and our policies.

In limited circumstances, we may require written consent to process certain particularly sensitive data. If we do so, we will provide full details of the information that we would like and the reason we need it, so that careful consideration may be given to whether you wish to consent.

Where we rely solely on consent as the lawful basis for processing, consent may be withdrawn at any time.

8. 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 safeguarding obligations, provided we do so in line with data protection legislation.

We envisage that we will hold information about criminal convictions, for example, if such information comes to light following a personal disclosure or Disclosure and Barring Service checks.

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.

9. Change of Purpose

We will only use your personal information for the purposes for which it was collected unless we reasonably consider that we need to use it for another reason, and that reason is compatible with the original purpose. Examples of compatible further use may include processing related to safeguarding, legal compliance, equality monitoring and the establishment, exercise or defence of legal claims.

If we need to use your personal data for a purpose incompatible with the purpose for which it was collected, we will notify you before we start the new processing. We will explain what we intend to do, 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 for which we collected it, 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***.

Following the recruitment process, we will retain your personal information and securely destroy it in line with our ***Data Retention Policy***.

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 ongoing incident/investigation which has been

identified (for example, if a crime has been observed and recorded or if the images have been retained while another subject access request is being processed). In such cases, images will be retained for as long as necessary (for example, until the conclusion of any criminal proceedings arising from the incident).

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

12. Data Sharing

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

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

- HR
- The recruitment/interview panel
- The line manager for the area with the vacancy
- IT manager, if access to the data is necessary for them to carry out their roles

If you are successful in being offered the post, the school will share your personal data with employment background check providers, the Disclosure and Barring Service and our Occupational Health provider to obtain necessary background, criminal records and health checks (see section 4 above).

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, accessed in an unauthorised way, altered, or disclosed.

Access to job applicant information is strictly controlled and aligned with the DUAA 2025 requirement, ensuring 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 employees, consultants, 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).
- Withdraw consent for 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 personal data for direct marketing
- Challenge processing, which has been justified based on public interest (in certain circumstances)
- Request a copy of agreements under which your personal data is transferred outside of the UK (if relevant)

- Object to decisions based solely on automated decision-making or profiling. The school **does not use** automated decision-making and/or profiling in any of its processes and procedures
- 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).

Your Duty to Inform us of Changes

The personal information we hold about you must be accurate and current. Please keep us informed if your personal information changes during the recruitment process.

Subject Access Requests (SAR)

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 for your own personal data it would be helpful if this could be made in writing to the Headteacher, including:

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

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 necessary for us to action your request without delay.

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 reissued.

Fulfilling A Subject Access Request

The lawful time frame for the School to respond to a Subject Access Request is one calendar month from receipt of a 'valid' SAR. 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 the School has limited staff resources outside of term time, we encourage job applicants to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays. This will help us respond to your request as promptly as possible.

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 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). For further information relating to your data subject rights, please see here: [Individual rights | ICO](#)

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 legitimate legal basis to do so.

16. Data Protection Complaints Process

Under the Data (Use and Access) Act 2025, individuals now have the right to raise a data-protection complaint directly with the School before contacting the Information Commission (ICO). A formal complaints process must be in place by 19 June 2026. In the meantime, if you wish to raise a concern about the handling of your personal data, you may contact the School directly, clearly stating the nature of the complaint and the desired resolution. For more information, please see here: [How to make a data protection complaint to an organisation | ICO](#)

School Contact Details

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

Data Controller's Representative: Nisha Gill, Headteacher. Email: head@cns.slough.sch.uk

Data Protection Officer: Dee Whitmore. Email: DPOService@schoolspeople.co.uk

17. 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 will provide you with a new Privacy Notice if we make any substantial updates. We may also notify you from time to time in other ways about the processing of your personal information.

Effective Date: May 2018

Last update: May 2026

Review Date: May 2027