POLICY DOCUMENT

Privacy Notice for the School Workforce

How Princess May Primary School collects and uses information about its employees, workers and contractors — 2026–2027

Governing Body Representative (GBR)	Kristofer McGhee (Chair of Governors)
Signed by (GBR)	……
Date approved	Awaiting governor approval (3 December 2026)
Next review due by	September 2027
Related policies	Data Protection Policy; Data Breach Policy; Data Retention Policy; Information Security Policy; CCTV Policy; Online Safety Policy
Aligned to	UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025; Judicium Education model privacy notice (September 2026)

This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

The UK GDPR operates alongside the Data Protection Act 2018, which supplements it by setting out additional provisions on matters such as the processing of personal data in specific sectors, exemptions, the powers of the Information Commission, and enforcement. The Data (Use and Access) Act 2025 further amends both the UK GDPR and the Data Protection Act 2018 to modernise UK data protection rules and clarify certain rights and obligations.

This notice applies to all current and former employees, workers and contractors.

1. Who Collects this Information

Princess May Primary School is a “data controller” of personal data and gathers and uses certain information about you. This means that we are responsible for deciding how we hold and use personal information about you. Under data protection legislation, we are required to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

2. Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our Data Protection Policy.

3. Categories of Information We Collect, Process, Hold and Share

Depending on your employment status, we may collect, store and use the following categories of personal information about you:

- Personal information and contact details, such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information, such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment, including references, proof of right to work in the UK, application form, CV and qualifications;
- Employment contract information, such as start dates, hours worked, post and roles;
- Education and training details;
- Details of salary and benefits, including payment details, bank details, payroll records, tax status information, National Insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information in your sickness and absence records, such as number of absences and reasons (including sensitive personal information regarding your physical and/or mental health);
- Criminal records information as required by law to enable you to work with children;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your time and attendance records;

- Information about the use of our IT, communications and other systems, and other monitoring information;
- Details of your use of business-related social media, such as LinkedIn;
- Images of staff captured by the school's CCTV system;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the school; you will be notified separately if this is to occur);
- Details in references about you that we give to others; and
- Recordings of staff from the school's video conferencing platform.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions;
- Trade union membership;
- Information about your health, including any medical condition and sickness records, details of any absences (other than holidays) from work including time on statutory parental leave and sick leave, and, where you leave employment for a reason related to your health, information about that condition needed for pension purposes;
- Information about criminal convictions and offences.

4. How We Collect this Information

We may collect this information from you in your application form, but we will also collect information in a number of different ways. This could be through the Home Office, our pension providers, medical and occupational health professionals we engage with, your trade union, the Disclosure and Barring Service (DBS), consultants and other professionals we may engage (for example, to advise us generally and/or in relation to any grievance, conduct, appraisal or performance review procedure), and other employees. Information is also collected through CCTV, access control systems and any IT system the school has in place, such as email, communication systems, remote access systems, instant messaging and voicemail.

5. How and Why We Use Your Information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests;
- When you have provided us with consent to process your personal data.

The situations in which we will process your personal information are listed below:

- To determine recruitment and selection decisions on prospective employees;
- To carry out effective performance of the employee's contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- To enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management, including retention, sickness and attendance;

- Performance reviews, managing performance and determining performance requirements;
- To manage internal policy and procedure;
- Human resources administration, including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks and the personal data of our employees, and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the school in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Further information on the monitoring we undertake in the workplace and how we do this is available in our Information Security Policy and Online Safety Policy.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

6. How We Use Particularly Sensitive Information

Sensitive personal information (defined under the UK GDPR as “special category data”) requires higher levels of protection and further justification for collecting, storing and using it. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our Data Protection Policy (for example, employment, social security or social protection obligations);
- For reasons of substantial public interest, such as for equal opportunities monitoring;
- To establish, exercise or defend legal claims;
- Where it is necessary to protect your vital interests (or those of another person) and you are unable to give consent.

We will use this information in the following ways:

- Collecting information relating to leave of absence, which may include sickness absence or family-related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting;
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

7. Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate, we will collect information about criminal convictions as part of the recruitment process, or we may be notified of such information directly by you in the course of working for us.

8. Sharing Data

We may need to share your data with third parties, including third-party service providers, where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

- The Department for Education (DfE);
- Ofsted;
- Prospective employers;
- Welfare services (such as children's social care);
- Law enforcement officials, such as the police and HMRC;
- The Local Authority Designated Officer (LADO);
- Training providers;
- Professional advisers, such as lawyers and consultants;
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The local authority (Hackney Education);
- Occupational health;
- The Disclosure and Barring Service (DBS); and
- Recruitment and supply agencies.

Information will be provided to those agencies securely and/or anonymised where possible. The recipient of the information will be bound by confidentiality obligations; we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

9. Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the school only retains personal data for as long as necessary to fulfil the purposes for which it was collected, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once you are no longer a member of staff at the school, we will retain and securely destroy your personal information in accordance with our Data Retention Policy, available on the Data Protection page of our website (www.princessmay.hackney.sch.uk/GDPR-POLICIES/).

10. Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach Policy and our Information Security Policy, which can be found on the Data Protection page of our website (www.princessmay.hackney.sch.uk/GDPR-POLICIES/).

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

11. Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are required to ensure that appropriate safeguards are in place when using automated decision making for significant decisions, and the circumstances in which we are permitted to use special category data (sensitive information) in automated decision making are limited.

You will not be subject to automated decision making for significant decisions unless we have a lawful basis, and a valid condition where required, for doing so and appropriate safeguards are in place. Appropriate safeguards include informing the relevant individuals about the automated decision making and their rights to request a human review, express their views, and contest the decision.

12. Your Rights of Access, Correction, Erasure and Restriction

Under certain circumstances, by law you have the right to:

- Access your personal information (commonly known as a “subject access request”). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example, for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact Marilyn Richards (Bursar), at admin@princessmay.hackney.sch.uk or on 020 7254 1589, in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

13. Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Marilyn Richards (Bursar), at admin@princessmay.hackney.sch.uk or on 020 7254 1589. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

14. Contact

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with Marilyn Richards (Bursar), at admin@princessmay.hackney.sch.uk or on 020 7254 1589, in the first instance. We will acknowledge receipt of your complaint within 30 calendar days, and we will investigate and respond without undue delay. Further information about the way we handle data protection complaints can be found in our Data Protection Policy, available on the Data Protection page of our website (www.princessmay.hackney.sch.uk/GDPR-POLICIES/).

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by Marilyn Richards, you can contact the DPO on the details below:

Data Protection Officer	Judicium Consulting Limited
Address	5th Floor, 98 Theobalds Road, London WC1X 8WB
Email	dataservices@judicium.com
Telephone	0345 548 7000
Web	www.judiciumeducation.co.uk

Should you remain dissatisfied with our response, you also have the right to make a complaint to the Information Commission (formerly the Information Commissioner's Office, ICO), the UK supervisory authority for data protection issues, at ico.org.uk.

15. Changes to this Privacy Notice

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. We may also notify you in other ways from time to time about the processing of your personal information.