Privacy Notice – Staff

Document owner: Manchester Hospital School

A: Leo Kelly School, 77 Dickenson Road, Manchester, M14 5AZ

T: 0161 509 2368 | E: admin@hospitalschool.manchester.sch.uk

Date: September 2026 | Review Date: September 2027

Introduction

The school must process your personal data to ensure that we can meet the terms of your employment contract and fulfil our legal and administrative obligations as an employer.

As part of our obligations under data protection law, namely the UK General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018, we must inform you how and why we process your personal data. The following privacy notice outlines what data we process about you as an employee, why we need it, and how it is used.

This privacy notice applies to all employees of the school, including those working with us on a temporary, supply, agency, or voluntary basis. For the purposes of this privacy notice, we refer to all such individuals as ‘employees’ or 'staff' of the school.

We ask that you review our ‘Data Protection Policy’ and 'Acceptable Use Policy' alongside this notice.

Data Controller

The school is the ‘Data Controller’ for the personal information that we process about you. This means that we are responsible for your data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection.

Our DPO is Danielle Eadie from RADCaT Ltd, who is supported by the senior leadership team (SLT) at the school. Any data protection queries should be forwarded to Carol Shaw, Assistant School Business Manager, via the school office in the first instance:

- **Contact:** Carol Shaw (Assistant School Business Manager)
- **Email:** admin@hospitalschool.manchester.sch.uk

- **Phone:** 0161 509 2368

The personal data that we process about you and why we need it

Recruitment & Induction

We process the following data about you to assess your suitability for the role, correspond with you during your employment, and meet the legal and statutory duties placed upon us by the Department for Education (DfE) workforce census:

- Personal identifiers: Name, address, and key contact details
- Next of kin and emergency contact details
- Special characteristics: Date of birth, gender/sex, religion, place of birth, and ethnicity
- Employment and education history
- Qualifications necessary for your role
- Personal statement and application details

The school conducts mandatory safer recruitment checks under statutory guidance (*Keeping Children Safe in Education*) to meet our safeguarding obligations. The following checks are conducted and logged on your record / Single Central Record (SCR):

- Identification checks (photo ID and proof of address)
- Enhanced Disclosure and Barring Service (DBS) check (and update service checks)
- Professional and character references
- Qualified Teacher Status (QTS) and teacher prohibition/management checks
- Right to Work checks / Visa status
- Online and social media searches as part of pre-employment screening
- Occupational health assessments (where relevant)

Contractual & Financial Information

The following information is processed to fulfil the terms of your employment contract with us and to administer the payment of your salary and benefits:

- Employment contract, job description, and salary scale
- Bank account details, National Insurance (NI) number, and tax codes
- Payroll records: salary, hours worked, deductions (e.g., trade union subscriptions), overtime, and expenses
- Statutory leave and absence records (e.g., sickness, maternity, paternity, adoption, shared parental, and flexible working requests)
- Pension enrolment details and benefit scheme records

Please note: For pensions and trade union deductions, the school only collects and transmits the necessary administrative data. The respective pension or union provider manages your contributions and membership records directly.

Performance, Professional Development & Management

We process the following information to monitor your performance, support your professional development, and manage operational matters:

- Performance reviews, appraisals, target setting, and contractual changes
- Training certificates and Continuing Professional Development (CPD) logs
- Disciplinary, grievance, or capability records where you are party or subject to proceedings
- Whistleblowing disclosures or investigation records

Health, Safety & Wellbeing

Employment and health & safety legislation requires the school to support workplace health and safety. We process:

- Occupational health referrals, reports, and agreed reasonable adjustments
- Health questionnaires and risk assessments (e.g., workplace, pregnancy, disability, or stress assessments)
- Fit notes and medical statements from healthcare professionals
- Accident logs, incident reports, and first-aid records

General Operational, Digital & Security Records

To maintain security, operational efficiency, and safeguarding:

- On-site attendance logs, visitor sign-ins, and trip logs
- System access, email, IT networks, and internet usage logs
- Staff ID badge photos
- CCTV footage
- Promotional photographs/videos (subject to explicit consent)

CCTV

Closed Circuit Television operates across the school site (internally and externally) for site security, safeguarding, and crime prevention. Footage may be reviewed to investigate serious misconduct, breaches of security, or health and safety incidents, and may be used in staff disciplinary procedures where necessary. Access is strictly restricted to designated personnel.

Monitoring – IT Usage, Digital Systems & Smart Glasses / Wearables

In accordance with statutory guidance (*KCSIE*), the school operates filtering and monitoring systems across all school network infrastructure, hardware, and connected digital accounts. Automated alerts notify designated leads of inappropriate searches, security risks, or prohibited site visits.

- **Smart Glasses and Personal Recording Equipment:** To protect pupil and staff privacy, maintain confidentiality, and ensure compliance with safeguarding policies, staff are strictly prohibited from wearing or using smart glasses, wearable devices with hidden camera/audio capabilities, or unauthorised recording equipment while on school grounds, in classrooms, or during confidential meetings.

- **Network Logs:** Usage logs and monitoring reports may be used as evidence in disciplinary investigations if a breach of the school's Acceptable Use Policy occurs.

Artificial Intelligence (AI) Where the school utilises software incorporating AI to support administrative processes or teaching, all data processed is anonymised, human oversight is maintained for all decisions, and no school data is used to train public or third-party AI models.

How we obtain your information

Most information is provided directly by you during application, onboarding, and throughout your employment. We also receive data from third parties, including previous employers (references), statutory checking bodies (DBS), government departments (HMRC, DfE), payroll providers, and medical professionals.

The lawful basis for processing personal data Under the UK-GDPR, we rely on the following lawful bases:

1. Legal Obligation: Meeting statutory requirements under:

- **Recruitment & Safeguarding:** *Keeping Children Safe in Education (KCSIE)*, UK Visa & Immigration Law
- **Health & Safety:** *Health & Safety at Work Act 1974*
- **Employment Law:** General UK Employment Legislation, *Equality Act 2010*
- **Statutory Returns:** *Education (Supply of Information about the School Workforce) (England) Regulations 2007* (DfE Workforce Census)

2. Contractual Necessity: To perform your contract of employment (e.g., paying your salary, administering pension contributions, managing leave).

3. Public Task: Carrying out tasks in the public interest (e.g., maintaining site security, delivering education, safeguarding pupils).

4. Legitimate Interests: To support school operations, manage IT accounts, and provide access to educational software and systems.

5. Vital Interests: To protect life or prevent serious harm in medical emergencies.

6. Consent: For optional activities (e.g., promotional photographs on the school website or social media).

Special Category Data

For sensitive data (e.g., health data, trade union membership, ethnicity, religious beliefs), we rely on additional conditions under **Article 9 UK GDPR** and the **Data Protection Act 2018 (Schedule 1)**:

- **Article 9(2)(b) UK GDPR (Employment, Social Security & Social Protection):** Fulfilling statutory employment duties, workplace safety, statutory sick pay, and equality monitoring.

- **Article 9(2)(g) UK GDPR (Substantial Public Interest):** Workforce census returns, equal opportunities monitoring, and serious safeguarding disclosures.
- **Article 9(2)(a) UK GDPR (Explicit Consent):** External health and occupational referrals where written consent is obtained.
- **Article 9(2)(c) UK GDPR (Vital Interests):** Disclosing life-saving medical details to emergency services.
- **Article 9(2)(f) UK GDPR (Legal Claims):** Establishing, exercising, or defending legal claims.

Storing and retaining your data

Staff records are kept securely in accordance with our *Records Management Policy & Retention Schedule*.

- **Personnel Files:** Maintained for the duration of employment plus 6 years post-employment.
- **Payroll & Tax Data:** Retained for 6 years from the end of the financial tax year to which they relate.
- **Safeguarding Records:** May be retained for longer periods in line with statutory guidance.

All electronic records are stored on encrypted, password-protected systems with multi-factor authentication (MFA) enabled. Physical files are stored in locked cabinets within restricted areas.

Sharing your personal information

We do not share staff data with third parties without consent unless permitted or required by law. We routinely share information with:

- The Local Authority and the Department for Education (DfE)
- HR and Payroll service providers
- IT infrastructure, management systems, and learning platform providers
- Pensions administrators and HMRC
- Occupational Health, NHS, and Wellbeing services (where applicable)
- External auditors, legal advisers, insurers, and regulatory bodies (e.g., Ofsted, HSE, ICO, Police)

Transferring data internationally

We do not routinely transfer personal data outside the UK. Any necessary international transfers via cloud providers comply strictly with UK GDPR requirements (e.g., UK Adequacy Regulations or International Data Transfer Agreements).

Requesting access to your personal data and your rights

Under data protection legislation, you have the right to:

- Access your data via a Subject Access Request (SAR)
- Request correction of inaccurate or incomplete data
- Request erasure or restriction of processing in specific circumstances
- Object to processing based on legitimate interests or direct marketing

- Withdraw consent at any time where processing is consent-based

To make a request, contact Carol Shaw, Assistant School Business Manager via the school office. Requests are processed within one calendar month.

Complaints

If you have any concerns regarding how your data is handled, please contact the school office in the first instance. You also have the right to complain directly to the Information Commissioner's Office (ICO):

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: https://www.ico.org.uk

Appendix 1: How the Government Uses Workforce Data

The school workforce data lawfully shared with the Department for Education (DfE) via statutory collections:

- Informs national policy on pay, workforce planning, and diversity monitoring
- Informs school funding allocations and expenditure models
- Supports long-term educational research and policy analysis

All data transferred to the DfE is handled under strict security controls. For further details on DfE data protocols or to submit a Subject Access Request directly to the DfE, please consult the DfE Personal Information Charter online at https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter