CHANCERY MULTI ACADEMY TRUST

Privacy Notice for School Workforce

Last Reviewed: November 2026
Next Review: November 2027

Introduction

Under UK data protection law, individuals have a right to be informed about how we collect and use their personal information. This privacy notice explains how and why the Trust collects, stores and uses personal information about current, former and prospective employees, workers, contractors, agency staff, apprentices and volunteers undertaking workforce duties within the Trust.

The Trust is the data controller for the purposes of UK data protection legislation.

The Categories of Personal Information We Process

We may collect, store and use the following categories of personal information:

Personal Information

- Name
- Title
- Date of birth
- Gender
- National Insurance number
- Employee number
- Teacher Reference Number (where applicable)
- Nationality and right to work information
- Home address
- Telephone numbers
- Personal and work email addresses
- Emergency contact details

Employment Information

- Job title and role
- Employment history
- Recruitment records
- Contracts of employment
- Start and leaving dates
- Working hours and employment status
- Performance management records
- Appraisal records
- Capability records
- Training and professional development records
- Disciplinary and grievance records
- Qualifications and certifications
- Subjects taught and curriculum responsibilities where relevant
- Attendance and absence information

Financial Information

- Payroll details
- Salary information
- Pension records
- Bank account details
- Tax information
- Expenses and reimbursement records

Safeguarding and Vetting Information

- Identity verification documents
- Disclosure and Barring Service (DBS) information
- Prohibition checks
- Right to work checks
- References
- Safeguarding records where applicable

Special Category Personal Data

Where necessary and lawful, we may process:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Health and medical information
- Disability information
- Equality monitoring information

Criminal Offence Data

Where permitted by law, the Trust may process information relating to criminal convictions, criminal offences and safeguarding checks.

Why We Collect and Use This Information

We collect and use workforce- information to:

- Recruit and appoint staff.
- Maintain personnel records.
- Pay staff and administer pensions.
- Manage contracts and employment relationships.
- Support and monitor professional development.
- Assess performance and conduct.
- Comply with safeguarding requirements.
- Monitor absence and wellbeing.
- Manage health and safety obligations.
- Ensure workforce planning and deployment.
- Meet statutory reporting requirements.
- Support equality, diversity and inclusion objectives.
- Defend or pursue legal claims.
- Comply with legal and regulatory obligations placed upon the Trust.

Our Lawful Basis for Processing

We process personal information under one or more of the following lawful bases under Article 6 of the UK GDPR:

Legal Obligation

Processing necessary for compliance with legal obligations, including:

- Employment law
- Education legislation
- Safeguarding legislation
- Health and safety legislation
- Tax and pension regulations

Public Task

Processing necessary for the performance of a task carried out in the public interest, including the provision of education and operation of state-funded schools.

Contract

Processing necessary to fulfil employment contracts and related obligations.

Legitimate Interests

In limited circumstances where processing is necessary for legitimate organisational interests and does not override individual rights and freedoms.

Consent

Where we rely on consent, individuals may withdraw that consent at any time.

Vital Interests

Where processing is required to protect life or prevent serious harm.

Processing Special Category Data

Where we process special category personal information, we do so in accordance with Article 9 of the UK GDPR and Schedule 1 of the Data Protection Act 2018.

This may include processing necessary for:

- Employment, social security and social protection obligations.
- Safeguarding children and vulnerable individuals.
- Occupational health purposes.
- Equality monitoring.
- Reasons of substantial public interest.
- Legal claims and regulatory compliance.

How We Collect Information

Most workforce information is collected directly from individuals through:

- Application forms

- Recruitment processes
- Employment contracts
- Payroll and pension documentation
- Staff declarations
- Performance management processes
- Training records
- Absence reporting processes
- Occupational health assessments

Information may also be received from:

- Previous employers
- Referees
- Recruitment agencies
- Disclosure and Barring Service
- Occupational health providers
- Regulatory bodies
- Local Authorities
- Government departments

Who We Share Information With

We may share personal information where necessary and lawful with:

- Schools within the Trust
- Local Authorities
- The Department for Education (DfE)
- Payroll providers
- Pension providers
- HM Revenue and Customs
- Occupational health providers
- Disclosure and Barring Service
- Teacher Regulation Agency
- Auditors and professional advisers
- Regulators and inspectors
- Software and ICT service providers
- Law enforcement agencies
- Courts and tribunals
- Professional bodies

We do not sell personal information.

Why We Share Workforce Information

We share workforce data to:

- Meet statutory reporting obligations.
- Support school workforce planning.
- Ensure payroll and pension administration.
- Comply with safeguarding duties.
- Deliver occupational health services.
- Meet regulatory requirements.
- Support audit, inspection and accountability arrangements.
- Maintain secure and effective educational provision.

Department for Education (DfE) Workforce Census

The Trust is required by law to provide workforce information to the Department for Education (DfE).

The workforce census is the mechanism through which workforce information is collected and shared with the DfE.

The information provided may include:

- Personal characteristics
- Qualifications
- Absence information
- Employment details
- Pay and contractual information
- Curriculum and teaching information where relevant

The DfE collects and processes workforce information under powers contained within education legislation and associated regulations.

How Government Uses Workforce Information

The workforce data that we lawfully share with the Department for Education may be used by the DfE to:

- Carry out its statutory functions.
- Inform education policy development.
- Support school workforce planning.

- Produce statistics.
- Undertake research.
- Monitor equality and diversity.
- Support funding decisions.
- Inform inspections and accountability arrangements.

The DfE may share information with approved organisations and researchers where permitted by law and subject to appropriate safeguards.

Further information regarding how the DfE uses personal information can be found on the GOV.UK website.

Storing and Retaining Information

The Trust retains workforce records in accordance with:

- UK legislation;
- The Information and Records Management Society (IRMS) retention guidance;
- Statutory safeguarding requirements; and
- The Trust's Records Retention Schedule.

Records are securely deleted, anonymised or destroyed when they are no longer required

---

International Transfers

Where personal information is transferred outside the United Kingdom, we will ensure appropriate safeguards are in place in accordance with UK data protection legislation.

This may include:

- UK adequacy regulations
- International Data Transfer Agreements
- Other approved transfer mechanisms

CCTV, Site Security and Digital Systems

The Trust takes the security of personal information seriously and has implemented appropriate technical and organisational measures to protect information against:

- Accidental loss;
- Unauthorised access;
- Unauthorised disclosure;
- Alteration; and
- Destruction.

Access to workforce data is restricted to authorised personnel who require access for legitimate business purposes.

The Trust also undertakes monitoring of its ICT systems, communications and security infrastructure. Further information can be found in Appendix 1: Monitoring of Trust ICT Systems, Communications and Security.

Your Rights

Under data protection legislation, individuals have the right to:

- Be informed about how their information is used.
- Request access to their personal information.
- Request correction of inaccurate information.
- Request completion of incomplete information.
- Request erasure of personal information in certain circumstances.
- Request restriction of processing.
- Object to processing in certain circumstances.
- Request transfer of information where applicable.
- Withdraw consent where processing is based on consent.
- Challenge decisions made solely by automated means (where applicable).

Not all rights apply in every circumstance and some exemptions may apply.

Subject Access Requests (SAR)

Individuals have the right to request access to personal information held about them.

Requests should be submitted to the Data Protection Officer using the contact details below.

Complaints

If you have concerns about how we use your personal information, please contact the Trust's Data Protection Officer in the first instance.

You also have the right to complain to the:

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Website: www.ico.org.uk
Telephone: 0303 123 1113

Data Protection Officer Contact Details

Jenny Whiston
dpo@chancerytrust.co.uk

Appendix 1: Monitoring of Trust ICT Systems, Communications and Security

Why We Monitor Trust Systems

To ensure the safety of pupils, staff and visitors, protect Trust information and assets, maintain the security of our ICT infrastructure and comply with our legal obligations, the Trust may monitor the use of its systems, networks and equipment.

This monitoring is undertaken in accordance with UK data protection legislation, safeguarding requirements, employment law obligations and the Trust's policies and procedures.

What May Be Monitored

When using Trust devices, systems, networks or accounts, the Trust may collect, record and review information relating to:

Communication Systems

- Trust email accounts
- Microsoft 365 applications
- Microsoft Teams communications
- Calendars and meeting records
- Shared mailboxes
- Telephone and VoIP systems
- Trust-approved messaging platforms

Network and Internet Usage

- Websites accessed
- Internet browsing activity
- Search activity undertaken on Trust devices
- Downloads and file transfers
- Device and user log-on information
- Network connection records
- Wi-Fi access logs

Device Monitoring

- Trust laptops, tablets and mobile phones
- Desktop computers
- Printing and scanning activity
- USB device usage
- Software installation records
- Security and antivirus logs

Building Access and Security Systems

- CCTV systems
- Door access systems
- Visitor management systems
- Entry and exit records
- Alarm and site-security systems

Safeguarding and Security Systems

- Web filtering records
- Monitoring and alerting software
- Cybersecurity logs
- Threat detection systems
- Malware protection systems
- Data loss prevention systems

Purposes of Monitoring

The Trust may monitor and process this information for the following purposes:

- Safeguarding children and vulnerable individuals.
- Protecting staff and visitors.
- Maintaining the security and integrity of Trust systems.
- Detecting and preventing cyber threats.
- Investigating safeguarding concerns.
- Preventing unauthorised access to systems.
- Detecting misuse of Trust equipment and networks.
- Preventing fraud and criminal activity.
- Ensuring compliance with Trust policies.
- Investigating disciplinary matters.
- Supporting business continuity and disaster recovery.
- Complying with legal, regulatory and audit requirements.

Lawful Basis for Monitoring

The Trust generally relies on one or more of the following legal bases:

- **Legal Obligation** - where monitoring is required by law or regulatory requirements.
- **Public Task** - where monitoring supports the Trust's public functions as an educational provider.
- **Legitimate Interests** - where monitoring is necessary to protect Trust systems, assets, information and users.
- **Vital Interests** - where monitoring is necessary to protect the life or safety of an individual.

Where special category data is incidentally captured through monitoring activities, the Trust will process such information in accordance with Article 9 UK GDPR and the Data Protection Act 2018.

Monitoring of Microsoft 365 and Cloud Services

The Trust uses Microsoft 365 and associated cloud-based services to support educational and operational activities.

As part of the administration and security of these services, authorised personnel may have access to:

- User account information.
- Login records.
- Audit logs.
- Security alerts.
- File access records.
- Email metadata.
- Teams usage information.
- Data-sharing and permissions records.

Access to such information is restricted to authorised staff and service providers acting on behalf of the Trust where necessary.

Safeguarding Monitoring

The Trust operates filtering and monitoring systems to help fulfil its safeguarding responsibilities.

These systems may:

- Record access to websites and online services.
- Identify potentially harmful or inappropriate online activity.
- Generate safeguarding alerts.
- Support investigations where safeguarding concerns arise.

Monitoring is proportionate and undertaken in line with statutory safeguarding duties and relevant guidance.

CCTV Monitoring

The Trust operates CCTV systems at some or all of its sites for:

- Crime prevention and detection.
- Site security.
- Protection of pupils, staff and visitors.
- Investigation of incidents.

Separate CCTV privacy information may be available where required.

Access to Monitoring Information

Access to monitoring records is restricted to individuals who require it for legitimate operational purposes, including:

- Senior leadership staff.
- Human resources personnel.
- Designated safeguarding leads.
- ICT and information security staff.
- Data protection personnel.
- External investigators, auditors or regulators where appropriate.

Information will only be accessed where there is a clear business, legal, safeguarding or security requirement.

Retention of Monitoring Records

Monitoring information will be retained only for as long as necessary in accordance with:

- The Trust's Records Retention Schedule.
- Information security requirements.
- Safeguarding obligations.
- Legal and regulatory requirements.

Retention periods may vary depending upon the nature of the information and any ongoing investigations or proceedings.

Employee Expectations

Users of Trust systems should not expect absolute privacy when using Trust-owned equipment, networks, email accounts or services for work-related purposes.

However, monitoring will be proportionate, lawful and undertaken only where there is a legitimate reason to do so.

The Trust will always seek to balance its operational, safeguarding and security requirements with the privacy rights of individuals.