



Privacy Notice for Employees



Under data protection law, 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 we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Glebe's DPO is John Moorhouse Data Protection Consultant Chorus Advisers and he is contactable through the GDPR lead (The Headteacher) who is contactable via office@glebeprimary.org.

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- A copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

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

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing workforce information are:

- Article 6 (1) (b) Contract: the processing is necessary because we have a contract with you and we need to process your personal information to comply with your contract
- Article 6 (1) (c) Legal obligation: the processing is necessary for us to comply with the law; we are required to share information about our workforce members under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments
- Article 6 (1) (e) Public Task: we may collect information from you where it is necessary to perform a task in the public interest e.g. taking temperature data on site and / or sharing staff data with the local authority in the event of a public health emergency
- Article 6 (1) (f) Legitimate interests: we rely on having a legitimate reason as your employer to collect and use your personal information, and to comply with our statutory obligations
- For some data processing where there is no legal obligation, contract or legitimate interest for the Trust to collect and use the data, we will ask for your consent under Article 6 (1) (a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose
- We may also share your information if we need to protect your vital interests (or someone else's interest) e.g. in a life or death situation we may share information with healthcare professionals

We will process special categories of personal data for lawful reasons only, including because:

- You have given us your explicit consent to do so, in circumstances where consent is appropriate
- It is necessary to protect your or another person's vital interests, for example, where you have a life threatening accident or illness in the work-place and we have to share your medical data in order to ensure you receive appropriate medical attention
- It is necessary for some function in the substantial public interest, including the safeguarding of children or vulnerable people, or as part of a process designed to protect others from malpractice, incompetence or unfitness in a role (or to establish the truth of any such allegations)

- It is necessary for the establishment, exercise or defence of legal claims, such as where any person has brought a claim or serious complaint against us or you

Public Health England also has special permission from the Secretary of State for Health and Social Care to use personally identifiable information without your permission where this is in the public interest. This is known as 'Section 251' approval and includes the use of the information collected by NHS Test and Trace to help protect the public from coronavirus. The part of the law that applies here is Section 251 of the National Health Service Act 2006 and the associated Health Service (Control of Patient Information) Regulations 2002. Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data. Where we have got your consent to use your data, you may withdraw this at any time. We will make this clear when we ask for your consent and explain how to go about withdrawing consent.

Why we use this data

The purpose of processing this data is to help us run the Trust, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing pupil information are to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

We have legitimate interests in processing the data - for example, where:

- You have applied for another position and references are required as part of safer recruitment
- Your marital status has changed and we are obliged to inform government office about this

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying) or whether you have a choice.

Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with the table below.

For your performance management, your performance manager will keep a hard copy in a file specific to you and an electronic version in their documents

Please see below for the type of records we keep and for how long for.

<u>Basic File Description</u>	<u>Retention Period</u>	<u>Action at end of the administrative life of the record</u>
Personnel file	Termination of Employment + 6 years, unless the member of staff is part of any case which falls under the terms of reference of IICSA. If this is the case then the file will need to be retained until IICSA enquiries are complete	SECURE DISPOSAL
Annual appraisal/assessment records	Current year + 6 years	SECURE DISPOSAL
Sickness absence monitoring	Sickness records are categorised as sensitive data. There is a legal obligation under statutory sickness pay to keep records for sickness monitoring. Sickness records should be kept separate from accident records. It could be argued that where sickness pay is not paid then current year + 3 years is acceptable, whilst if sickness pay is made then it becomes a financial record and current year + 6 years applies. The actual retention may depend on the internal auditors. Most seem to accept current year + 3 years as being acceptable as this gives them, 'benefits' and Inland Revenue have time to investigate if they need to	SECURE DISPOSAL
Absence request	3 academic years	SECURE

forms		DISPOSAL
Staff training – where the training leads to continuing professional development	Length of time required by the professional body	
Staff training – except where dealing with children, e.g. first aid or health and safety	This should be retained on the personnel file. Date of the training + 40 years [This retention period reflects that the IICSA may wish to see training records as part of an investigation]	
Records relating to any allegation of a child protection nature against a member of staff	Until the person's normal retirement age or 10 years from the date of the allegation (whichever is the longer) then REVIEW. Note: allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned UNLESS the member of staff is part of any case which falls under the terms of reference of IICSA. If this is the case then the file will need to be retained until IICSA enquiries are complete	SECURE DISPOSAL
Disciplinary proceedings <ul style="list-style-type: none"> • oral warning • written warning • final warning • case not found 	date of warning + 6 months date of warning + 12 months date of warning + 18 months If the incident is related to child protection then see above, otherwise dispose of at the conclusion of the case	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
Reports created by the Head Teacher or the Management Team	Date of the report + a minimum of 3 years then review annually or as required if not destroyed	SECURE DISPOSAL
Records created by senior leaders and other members of staff with administrative responsibilities which do not fall under any other category	Current academic year + 6 years then review annually, or as required if not destroyed	SECURE DISPOSAL
Correspondence created by senior leaders and other members of staff with administrative responsibilities	Current year + 3 years	SECURE DISPOSAL
Professional development plans	These should be held on the individual's personnel record. If not then termination of employment + 6 years	SECURE DISPOSAL
school development plans	Life of the plan + 3 years	
All records leading up to the appointment of a headteacher	Unsuccessful attempts. Date of appointment plus 6 months. Add to personnel file and retain until end of appointment + 6 years, except in cases of negligence or claims of child abuse then at least 15 years	SECURE DISPOSAL
All records leading up to the appointment of a member of staff/governor – unsuccessful candidates	Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
Pre-employment vetting information – DBS Checks – successful candidates	DBS Update Service Employer Guide June 2014; Keeping Children Safe in Education. 2022 (Statutory Guidance from DoE) Sections 73, 74	SECURE DISPOSAL

Forms of proof of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Where possible this process should be carried out using the on-line system. If it is necessary to take a copy of documentation then it should be retained on the staff personnel file.	SECURE DISPOSAL
Pre-employment vetting information – Evidence proving the right to work in the United Kingdom – successful candidates	Where possible these documents should be added to the staff personnel file , but if they are kept separately then the Home Office requires that the documents are kept for termination of employment + not less than 2 years	SECURE DISPOSAL
DBS Application forms	Number to be retained on Single Central Register but not the copy of the certificate	
Trainee Teacher records	All copies to be deleted at end of placement and submission of final report; except final report to be kept by mentor / HT for 3 years (may be required for references) and then deleted.	SECURE DISPOSAL
Accident / incident report	Yes 7 years after incident for adults; 25 years after birth for children	
Evolve School Trip Records including trip risk assessments, adults attending and pupil lists	Paper copies to be shredded on return except copy in EVC coordinator’s office to be kept for one year.	DELETED BY EVOLVE SHRED / DELETE

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

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

- *Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns*
- *The Department for Education – to meet our legal obligations to share certain information with it, such as teacher qualifications*
- *Your family or representatives – to meet our vital interests obligation to share information with your family or representative in an emergency situation, such as an accident at work*
- *Our regulator: Ofsted – to meet our legal requirement to share certain information with it, such as the staffing structure*
- *Suppliers and service providers – to enable them to provide the service we have contracted them for, such as music lessons*
- *Financial organisations – to meet our legal obligation to share certain information with it, such as the staffing structure*
- *Our auditors – to meet our legal obligation to share certain information with it, such as payroll information*
- *Survey and research organisations- to meet our legal obligation in relation to ‘freedom of information’ requests*
- *Trade unions and associations- to carry out our public task in light of any key discussions within school linked to disciplinary/capability procedures or for events such as redundancy.*

- Security organisations- in order to keep our school secure and under the lawful basis of public task, we pass on certain staff member information so that they can be contacted if necessary (such as the caretaker).
- Health and social welfare organisations to carry out our public task in line with our attendance management policy with organisations such as occupational health
- Police forces, courts, tribunals- to meet our legal obligations to share certain information with it, such as safeguarding concerns or to carry out our public task in relation to a tribunal.
- Employment and recruitment agencies- to meet the public task of supplying requested references.
- The governors- to carry out our public task within the school and remain accountable to them for finance and personnel issues.
- Professional bodies – to meet our contractual obligation to share information with it such as, residential trips
- Security organisations – to meet our vital interests to ensure that staff and pupils are safe, for example CCTV images

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law and ensure that the legal framework in place in that country, territory, sector or international organisation provides 'adequate' protection for individuals' rights and freedoms for their personal data.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

John Moorhouse
 Chorus Advisors Ltd
 University of Essex,
 4th Floor Gateway Building,
 Southend-On-Sea,
 Essex SS1 1LW,
 United Kingdom

