

GDPR Privacy notice for Employees

What is the purpose of this document?

Epworth Education Trust is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR). It applies to all employees.

Epworth Education Trust is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold and process about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and process the following categories of personal information about you:

Information related to your employment:

We use the following information to carry out the contract we have with you, provide you access to services required for your role and manage our human resources processes. We will also use it for our regulatory purposes in our role as an academy trust and to fulfil our role of promoting openness by public bodies and data privacy for individuals.

- *Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.*
- *Date of birth, gender and NI number*
- *Your photograph*
- *A copy of your passport, driving license or similar photographic identification and proof of address documents.*
- *If required, your electronic signature when you sign off documents*

- *Marital status and dependants*
- *Next of kin and emergency contact information*
- *Recruitment information (including copies of right to work documentation, references, qualification certificates, job application, CV or cover letter, details of any criminal convictions that you declare, and any other information collected as part of the application process).*
- *Details of any secondary employment, conflict of interest declarations or gift declarations.*
- *Reference requests and copy of data given*
- *Your responses to staff surveys if this data is not anonymised*
- *Any content featuring you, produced for use on our website, intranet or social media such as photos, videos, newsletter article, training webinars if consent given.*

Information related to your salary, pensions and loans:

We process this information for the payment of your salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday and maternity leave.

- *Information about your job role and employment contract including your start and end date, salary (including grade and scale point), contract variations, working patterns.*
- *Details of your time spent working and any overtime, expenses or other payments claimed.*
- *Flexible working requests*
- *Bank account details, payroll records and tax status information*
- *Pension details including membership of both state and occupational schemes (current and previous) and your contributions*
- *Salary sacrifice schemes and other loans*
- *and benefits information*
- *Location of employment or workplace*
- *Leave of Absences including sick leave, holidays, special leave*
- *Details relating to Maternity, Paternity, Shared Parental, and adoption leave including applications, MATB! Forms and any other relevant documentation.*
- *Trade union membership for the purpose of the deduction of subscriptions directly from salary for which you have given consent to the data controller (the union)*
- *Compensation history*

Information related to your performance and training:

We use this information to assess your performance, to conduct Professional Learning Reviews and to deal with any employer-employee related disputes. We also use it to meet the training and development needs required for your role.

- *Performance at work information eg. Probation reviews, PLRs, promotions*
- *Grievance and dignity at work matters and investigations to which you may be party or witness.*
- *Disciplinary records and documentation related to any investigations, hearings and warnings or penalties issued.*
- *Whistleblowing concerns raised by you, or to which you may be part or witness.*
- *Information related to your training history and development needs.*
- *Professional memberships*
- *Leadership development profiles*
- *Audio and video from any training or observation sessions you attend that are being recorded with your consent*

Information relating to monitoring:

We use this information to assess your compliance with your contract, corporate policies, and procedures and to ensure the security of our premises, IT systems and employees.

- *Photos*
- *CCTV footage (where audio capability is a function, this will be turned off)*
- *Information derived from monitoring Epworth Education Trust staff IT acceptable use standards as per the policy.*
- *Electronic and paper-based signing in systems*
- *Technologies for monitoring timekeeping or access control*
- *Information about your use of our information and communications systems*

Information relating to your health and wellbeing and other special category data

We use the following "special categories" of more sensitive personal information to comply with legal reporting under employment and health and safety law, our legal obligations under an employment contract and for equal opportunities monitoring. We also use it to ensure the health, safety, and wellbeing of our employees. There may on rare occasions legitimate interest in sharing health information with our solicitors to obtain appropriate legal advice or to defend legal claims.

- *Health and wellbeing information either declared by you voluntarily or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, pre-employment medical checks and fit notes i.e. Statement of Fitness for Work from your GP or hospital.*
- *Accident records if you have an accident at work including Riddor Reportable*
- *Details of any desk audits, access needs or reasonable adjustments.*
- *Information you have provided regarding Protected Characteristics as defined by the Equality Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics.*
- *Genetic information and biometric data*
- *Health data with only be shared with our Occupational Health advisors on employee consent.*

Data protection law requires the employer to ensure personal information is accurate and kept up to date (the accuracy principle). Therefore, Epworth Education Trust will take all reasonable steps to ensure our employees' health information is not incorrect or misleading and is kept updated where health information such as hearing levels could change over time. Employees will be asked periodically to check their medical information is accurate.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- *Making a decision about your recruitment or appointment.*
- *Determining the terms on which you work for us*
- *Checking you are legally entitled to work in the UK*
- *Paying you and, if you are an employee, deducting tax and National Insurance contributions.*
- *Providing the following benefits to you: Employer Pension scheme, staff wellbeing plan which includes the employee assistance programme as well as other plans that may be available such as the GP helpline, optical eyecare vouchers and occupational health assistance.*
- *Liaising with your pension provider*
- *Administering the contract we have entered into with you*
- *Business management and planning, including accounting and auditing*

- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- Equal opportunities monitoring to monitor our compliance with the Public Sector Equality Duty
- To carry out the School workforce census to enable the development of a comprehensive picture of the workforce and how it is deployed
- To use in marketing literature (with your consent)

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

How is your personal information collected?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. We will collect additional personal information during job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Depending on the processing activity, we rely on the following lawful basis for processing your data under the UK GDPR.

1. Where we need to perform the contract, we have entered into with you (Article 6(1)(b))
2. Where we need to comply with a legal obligation e.g. Education Act 1996 (Article 6(1)(c))
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests (Article 6(1)(f))
4. Where we need to protect your vital interests (or someone else's interests. (Article 6(1)(d))
5. Where it is needed in the public interest [or for official purposes (Article 6(1)(e))

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations and in line with our Data Protection policy
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our Data Protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

If you fail to provide 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 (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

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. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal 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 obligations and provided, we do so in line with our Data protection policy.

Law enforcement authorities are subject to the separate law enforcement regime under Part 3 of the DPA 2018, so less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members during legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

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 once the applicant has been shortlisted or we may be notified of such information directly by you during you working for us. We will use information about criminal convictions and offences in the following ways:

- To carry out our obligations by ensuring you are not putting any of our children and employees at a safeguarding risk within with-in the workplace

- To ensure we have minimised our risk of fraud within the workplace

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including our data processors, training providers, solicitors, legal advisors, government agencies and external auditors.

In some circumstances such as a court order or under the Public Records Act 1958, we are legally obliged to share information.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We do not routinely transfer staff personal data overseas but when this is necessary, we ensure that we comply with UK GDPR, ensuring appropriate safeguards are in place.

Why might you share my personal information with third parties?

We will share your personal information with third parties 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.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group as well as data processors can be found at **Annex A**

School workforce census

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trust) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to:

- <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.
- The department may share information about school employees with third parties who promote the education of well-being of children or the effective deployment of school staff in England by:
- Conducting research or analysis

- Producing statistics
- Providing information, advice and guidance
- The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:
 - Who is requesting the data
 - The purpose for which it is required
 - The level and sensitivity of data requested; and
 - The arrangements in place to securely store and handle the data
- To be granted access to school workforce information, organisations must comply with its strict terms and condition covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
- For more information about the department's data sharing process, please visit:
 - <http://www.gov.uk/data-protection-how-we-collect-and-share-research-data>
 - To contact the department: <https://www.gov.uk/contact-dfe>

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on performance, in the context of a reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of a restructure of the business, takeover, merger or academy sponsorship. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

Both Physical and electronic records are held for each member of staff. Data is held securely on our IT systems and at the Trust and/or school premises.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. 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. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from Joanne Buckley.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Retention policy and CCTV policy (if relevant for your school). To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy and applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

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.

Your rights in connection with personal information

As an individual you have certain rights regarding our processing of your personal data, including a right to lodge a complaint with the Information Commissioner as the relevant supervisory authority.

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

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want 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 Joanne Buckley in writing.

No fee usually required: You will not have to pay a fee to access your personal information (or to exercise any of the other rights). 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.

What we may need from you: 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). This is another appropriate security measure to ensure that personal information is not disclosed to any person

who has no right to receive it.

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 Joanne Buckley in writing. 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.

Data Protection Officer

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

The Data Protection Officer is **Joanne Buckley**

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.

If you have any questions about this privacy notice, please contact Joanne Buckley on 07554421471.

Annex A

Data Processor	Purpose	Privacy Policy
IMP budgeting software	Budgeting software provider	Privacy Policy - IMP Software Privacy Policy
PS financials (Iris)	Financial	Privacy Policy IRIS Software Group
Safesmart Smartlog	Training provider	Privacy Policy Safesmart
Inventry	Visitor management and sign-in solution to manage visitors, staff, pupils and contractors.	InVentry Sign-In System GDPR Policies & Frequently Asked Questions
Arbor	Cloud-based management information system (MIS) used for pupil and staff information	Privacy Notice & Cookie Statement - Arbor (arbor-education.com)
SIMS	Management information system (MIS) used for pupil and staff information	Privacy Notice Education Software Solutions
SAS staff insurance	Staff insurance	privacy-notice.pdf (sas-offload-uploads.s3.eu-west-2.amazonaws.com)
Microsoft	Microsoft 365 package inc teams	Privacy – Microsoft privacy
Hill Dickinson	Legal services provider	Privacy notice Hill Dickinson
Moore and Smalley	Provider of accounting and auditing services	Moore-and-Smalley-Privacy-Statement-August-2023.pdf (mooreandsmalley.co.uk)
Teachers Pension	Pension Scheme for teachers	Privacy Teachers' Pensions (teacherspensions.co.uk)
Derbyshire pension scheme	Pension Scheme for staff	Privacy policy - Derbyshire Pension Fund
Greater Manchester pension scheme	Pension Scheme for staff	Data protection - GMPF
Merseyside Pension Fund	Pension Scheme for staff	Privacy Notice for the members and beneficiaries of Merseyside Pension Fund Merseyside Pension Fund (mpfmembers.org.uk)
Lancashire Pension Fund	Pension Scheme for staff	Privacy notice - Lancashire County Council
Dojo	Communication app for teachers, parents, and students.	Privacy Policy ClassDojo
Ofsted	Inspect and regulate educational services	Privacy statement - Find an Inspection Report - Ofsted
Cpoms	Software to manage and monitor safeguarding, pastoral and welfare concerns for pupils.	Privacy Notice (cpoms.co.uk)
Tapestry (foundation stage forum)	Eyfs assessment Tool for practitioners	Privacy Policy Tapestry
Parentpay		Privacy Notice - ParentPay Cookie Policy How We Use Cookies ParentPay
Parentmail	Online payment and communication service for	privacy-policy.pdf (parentmail.co.uk)

	parents, students, and staff.	
Evolve (edufocus)	Online management tool, system for the planning, approval and management of educational visits, sports fixtures and extra-curricular activities.	eduFOCUS Privacy Policy
Techscheme/Cyclescheme	Salary sacrifice scheme for staff	Privacy policy Blackhawk Network
Smartclinic occupational health	Occupational health advisers	Data Policy 2024 (smartclinic.com)
Orian schoolhub	Catering provider for Wigan schools	Privacy Policy — Orian Solutions
Abtec	IT support for Wigan schools	
Juniper education	Website provider	Privacy Policy (junipereducation.org)
Edupay	Payroll and HR services provider and software	Awaiting
All Local Authorities – Bury Derbyshire Lancashire Oldham St Helens Tameside Wigan		Privacy Notice - Bury Council Website privacy policy - Derbyshire County Council Privacy notice - Lancashire County Council Data protection and freedom of information / Oldham Council Privacy policy - St Helens Borough Council Tameside Metropolitan Borough Council Data Protection Privacy Notice Privacy policy (wigan.gov.uk)
Counsellor??		