Privacy Notice:
Trust Workforce

For public viewing

Link to other policies and notices:

- Coronavirus Track &Trace
- Data Protection Policy
- CCTV Policy
- Data Retention Policy & Schedule
- Subject Access Request Policy
- Data Security Policy
- Data Handling Policy & Procedure

Zest Academy Trust, Waterloo Road, Blackpool, FY4 3AG
T 01253 315370 F 01253 316493 E admin@zestacademytrust.co.uk W www.zestacademytrust.co.uk

CEO Mr M Hamblett

Registered in England No. 8087508 Company Limited by Guarantee VAT Reg No. 000 0000 00

Zest Academy Trust
Privacy Notice – Workforce

Contents

Introduction

Under data protection law, individuals have a right to be informed about how the Trust 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 for the Trust.

We, Zest Academy Trust are the 'data controller' for the purposes of data protection law. The Trust is registered as a data controller with the Information Commissioners Office (ICO). Our registration number is Z3239207

This Privacy Notice relates to Zest Academy Trust, its Academy – Waterloo Primary Academy and any other Academy which joins the trust in the future (hereafter referred to as the 'Trust').

Our data protection officer is The Schools People (see 'Contact us' below).

1. Data Protection Principles

Personal Data must be processed in accordance with the six Data Protection Principles. It must be:

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

2. The Types of Personal Data We Collect

We process data relating to those we employ, or otherwise engage, to work For the Trust. Personal data that we may collect, use, store and share (when appropriate) may include, but is not restricted to:

- Personal details including name, address, contact details including email and telephone number, date of birth, nationality, marital status and gender
- Next of kin, dependants, emergency contact numbers
- Salary, annual leave, pension and benefits information such as pensions and insurance cover
- Bank account details, payroll records, National Insurance number and tax status information, pension contributions, other deductions, student loans, timesheets.
- Recruitment information, including copies of Right to Work documentation, DBS Checks and Children's Barred List information, Overseas check, Teacher status checks.
- Employment references and other information included in a CV, 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, start date, post, roles and continuous service data
- Performance management information including appraisals, performance reviews and ratings, performance improvement plans and related correspondence
- Outcomes of any disciplinary and/or conduct/grievance procedures including warnings and related correspondence
- Settlement agreements, COT3 agreements, and claims to an Employment Tribunal or Employment Appeal Tribunal
- Leave data including holidays, family leave and sabbaticals
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the Trust's information and communications system
- Any other personal data we will inform you of from time to time

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, disabilities, reasonable adjustments and sickness absence records, GP details, medical records (where appropriate), OH referrals and reports
- Criminal record (see section 7 below)

3. How we Collect This Data

We collect employee personal data from: -

- CVs and job application forms, and the recruitment process, either directly from individuals or indirectly via employment agencies.
- Third parties including references from previous employers, the Local Authority or other agencies (e.g. DBS Checks)
- identity documents including passport and driving license
- data collection forms completed by you at the start of, and during the course of your employment with the Trust
- health providers such as Occupational Health and Fitness to Work notifications; and,
- During the course of your employment including attendance records, sickness records, performance reviews and complaint/disciplinary/grievance investigations, correspondence, meetings or other assessments.

While the majority of information we collect about employees is mandatory, there is some information that may be provided voluntarily.

Whenever we seek to collect information from employees, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying. If you fail to provide certain information when requested, we may be prevented from complying with our official or legal obligations (e.g. such as paying you).

4. Why We Collect and Process This Information

We collect personal data to enter into a contract with you, to safeguard our stakeholders, promote the objects and interests of the Trust, facilitate the efficient operations of the Trust and to ensure that all relevant legal obligations of the Trust are complied with.

For example, we collect data to:

- facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Trust complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- allow better financial modelling and planning
- provide a safe working environment through using current medical data to minimise risk and safeguard staff
- provide references on request for current or former employees; and
- respond to and defend against legal claims.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations such as those in relation to employees with disabilities.

Where the Trust processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for equal opportunities monitoring and to carry out its obligations and exercise specific rights in relation to employment.

5. Automated Decision Making

Automated decision-making takes place when an electronic system uses personal information to make decisions without human intervention. We are permitted to use automated decision-making in limited circumstances.

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.

6. Our Lawful Basis for Using This Data

We only collect and use personal data when the law and our policies allow us to do so. We process general category data where:

- The data subject, or a person with the lawful authority to exercise consent on the data subject's behalf, has given explicit consent
- Processing is necessary for a contract, we have with you, or because it is necessary to take steps before entering into a contract with you
- Processing is necessary for us to comply with a legal obligation.
- Processing is necessary to protect your vital interest or that of another person.
- Processing is necessary for us to perform a task in the public interest or for our official functions, and this task or function is lawful

We process special category data where:

- The data subject, or a person with the lawful authority to exercise consent on the data subject's behalf, has given explicit consent
- Processing is necessary for carrying out our obligations in relation to employment law
- Processing is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent
- The processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- Processing is necessary, where applicable, for preventative or occupational medicine to assess the working capacity of the employee or to obtain a medical diagnosis
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Some of the reasons listed above for collecting and using personal data overlap, and there may be several grounds which justify our use of this data.

7. Criminal Proceedings/Convictions

We may only use information relating to criminal convictions where the law allows us to do so. Th**is** will usually be where such processing is necessary to carry out our obligations and provided that we do so in line with the data protection legislation.

We envisage that we will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of our appointment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your time as an employee.

Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and/or the Police. Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the data secure.

8. CCTV

We use CCTV in various locations around the Trust site. The purpose of the system is to prevent crime and promote security and public safety. If in the event of viewing CCTV for the specified purpose, a safeguarding or criminal action is observed, the CCTV can and may be used to support any subsequent investigation.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

CCTV images will be retained for 21 days. After this period images will be permanently deleted unless they are required and retained for an ongoing investigation. For example, if an incident or crime has been recorded. In such cases, the images will be retained until the conclusion of any actions or criminal proceedings arising from the incident.

For more information about the Trust's use of CCTV please refer to ***CCTV Policy***

Any enquiries about the CCTV system should be directed to the ICT Manager.

9. Consent

We may process your personal information without your knowledge or consent, in compliance with the above lawful bases where this is required or permitted by law and our policies.

We will ask for consent to process personal data where there is no other lawful basis for processing it. For example, if we need to obtain an Occupational Health Report and/or access to your medical records, or we wish to use your photograph in promotional/marketing materials. If we do request your consent, 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.

10. Change of Purpose

We will only use your personal information for the purposes for which it was collected 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, or seek your consent if necessary, prior to the processing.

11. Data Storage and Retention

A significant amount of personal data is stored electronically. Some information may also be stored as hard copy.

All data stored and accessed is done so in accordance with the Trust's ***Data Security Policy*** and ***Data Handling Policy and Procedure.***

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, insurance or reporting requirements. Details of retention periods for different aspects of your personal information are available in our ***Data Retention Policy and Schedule***.

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.

When your time as an employee with the Trust comes to an end, we will retain and securely destroy your personal information in accordance with our ***Data Retention Policy and Schedule***.

12. Sharing Personal Data

We do not share employee data with anyone without consent unless the law and our policies allow us to do so. We routinely share employee data with:

- The Local Authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- The Department for Education - to fulfil our statutory reporting requirements.

<u>Department for Education</u>

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our workforce with the Department for Education (DfE) for the purpose of those data collections, under:

We are required to share information about our school employees with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see '*How Government uses your data*' section below.

From time to time, we may also share Trust workforce information with other organisations including:

- the Department for Education (DfE)
- School Governors
- Disclosure & Barring Service
- Our regulators [e.g. Ofsted, SIAMS]
- Central and local government
- Police forces or other law enforcement agencies, courts, tribunals
- The Teaching Regulation Authority
- Prevent teams in accordance with the Prevent Duty on schools
- Your Trade Unions and associations
- Your family or representatives
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Professional bodies

Other third-party service providers

We also share limited personal data with third-party service providers who require access to data in order to perform contracted services. These service providers include:

- Professional advisers and consultants (e.g HR Consultancy, DPO Services)
- Payroll
- Capita Sims to facilitate database administration and technical support
- Legal advisors and Insurance providers
- IT providers
- Occupational Health provider
- Wellbeing Service provider
- Teacher Pensions/Local Government Pensions
- HMRC
- Any other third-party service provider we will inform you of from time to time

These third-party service providers act as data processors on the Schools behalf and are required to take appropriate security measures to protect your personal information in line with our policies and data protection legislation. We authorise these service providers to use personal data only as necessary to perform services on our behalf, or to comply with legal obligations if necessary.

13. Transferring Data Outside the European Economic Area (EEA)

We do not routinely share data with organisations outside the EEA. Where this may be necessary, e.g. where a former employee has emigrated and/or applied to work outside the EEA, data may be transferred to the new employer with explicit consent from the former employee and with appropriate safeguards.

Under exceptional circumstances, we will only transfer personal data outside the European Economic Area (EEA) if such transfer complies with the GDPR. This means that we will not transfer any personal data outside the EEA unless:

- The EU Commission has decided that another country or international organisation ensures an adequate level of protection for personal data
- One of the derogations in the GDPR applies (including if an individual explicitly consents to the proposed transfer).

14. Data Security

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, consultants, 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.

We have 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 and in accordance with our ***Data Security Policy and Breach Procedure***.

15. Your Data Subject Rights

Under data protection legislation you have the right to:

- Make a Subject Access Request (SAR) (see below)
- Withdraw your consent to the processing at any time
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it (in certain circumstances)
- Prevent use of your personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which your personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling. (See section 5 above)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Your Duty to Inform us of Changes

The personal information we hold about you must be accurate and current. Please keep us informed if your personal information changes during the recruitment process.

Subject Access Requests

Under data protection legislation, individuals have the right to request access to their personal data held by the Trust. Subject Access Requests ***may be*** made to the Trust in written form or verbally.

If you would like to make a SAR in relation to your own personal data it would be helpful if this could be made in writing to the Headteacher, including:

- name and contact address
- email address and telephone number
- details of the information required.

A helpful '***Guide to Making A Subject Access Request***' is available from the office, or as a download from the website. It ***is not*** mandatory to make a Subject Access Request using the form. It will, however, assist you in structuring your SAR to provide the information necessary to ensure we can action your request without delay.

Fulfilling A Subject Access Request

The lawful time scales for the Trust to respond to a Subject Access Request is one calendar month from receipt of a '**valid**' SAR.

A SAR is only considered '***valid***' when we are fully satisfied regarding the identity of the requester and their entitlement to the data requested. If in any doubt we will request confirmation of identity to ensure your personal data is not inadvertently released to a third-party who is not entitled to it.

If the SAR is complex or numerous, the period in which we must respond may be extended by a further two months. You will be notified of any delays in actioning the SAR and provided with a timeframe in which you can expect to receive the requested data.

Fees

You will ***not*** have to pay a fee to access your personal information (or to exercise any of your other data subject rights). However, we may charge a reasonable fee if your access request is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Exercising Other Data Subject Rights

If you wish to review, verify, correct or request the 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 the Trust in the first instance (details below).

The Right to Withdraw Consent

Where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, and there is no other applicable lawful basis for processing the data, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Nicola Lea (please see section 17 contacts below).

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.

16 Complaints

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

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

If you have any concerns that we are not able to resolve to your satisfaction you can contact our Data Protection Officer at the address below

Alternatively, you can register your concern with the UK's data protection regulator - the Information Commissioner's Office:

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

17. 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

Data Protection Officer: The Schools People
Email: DPOService@schoolspeople.co.uk
Tel: 01773 851078
Address: The Schools People
44 Tyndall Court
Peterborough
PE2 6LR

Data Controller: Zest Academy Trust
C/O Waterloo Primary Academy
Waterloo Road
Blackpool
Lancashire
FY4 3AG

Data Controllers Representative: Mrs Nicola Lea
Email: hr@zestacademytrust.co.uk
Tel: 01253 600656

18. Changes to this Privacy Notice

This Notice will be reviewed on a yearly basis or as necessary in relation to changes in Data Protection legislation.

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.

Effective Date: January 2020
Last update: January 2020
Review Date: January 2021

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs government policy on matters related to child and family social workers
- may be used to inform the distribution of funding to local authorities
- supports 'longer term' research and monitoring of children's social care policy

Data collection requirements

Sharing by the Department

The Department may share information about employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or 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 workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:
https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: https://www.gov.uk/contact-dfe