Employee Privacy Notice:

How we use your information

This privacy notice was updated on 13 July 2020

Personal information we collect

We collect the following information about you:

- Personal identifiers (such as your name, date of birth, employee or teacher number, national insurance number, car registration number)
- Characteristics information (such as gender, age, ethnic group)
- Recruitment information (e.g. job application; qualifications, training and education, evidence of your right to work, references)
- Contract information (such as start date, hours worked, post, roles, salary and bank details, pension and tax information)
- Personnel information (such as appraisal and performance)
- Work absence information (such as number of absences and reasons, fitness to work and occupational health information)
- Outcome of your Disclosure and Barring Service (DBS) check and certificate number
- Health, disability or dietary requirements you have chosen to share with us
- Next of kin and emergency contacts
- Religious or other beliefs
- Allegations or concerns about child protection or safety
- Fingerprints to enable you to use our cashless catering, library or ICT services
- Photographs and video recordings of you (such as official school photographs, classwork activities, performances or events, school trips and sports days)
- Your image captured on our CCTV system when you are on school premises
- Your facial image captured on our electronic visitor management system
- Your consent preferences

We need this information to:

- Recruit, retain, train, appraise, manage the welfare of and performance of staff
- Enable individuals to be paid, pension contributions made, and tax and NI deducted
- Undertake our responsibilities for safeguarding children
- Provide employee services and benefits (such as childcare vouchers and pensions)
- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Communicate with employees regarding work related matters
- Comply with the law regarding data sharing
- Maintain staff records
- Provide catering, payment, library, ICT, learning and information services
- Assess the quality of our services
- Assist in crime prevention, detection and public safety
- Carry out audits (e.g. to ensure compliance with our legal obligations)
- Deal with complaints, grievances and disciplinary action
- Complete DfE school workforce census
- Administer school trips and activities
- Monitor and comply with our responsibilities under the Equality Act 2010 and make reasonable adjustments where required
- Safeguard and monitor the health and welfare of our employees
- Ensure staff and student safety and security

Who we share information with

We share information with a range of organisations, companies and agencies, where it is necessary for us to carry out our legal responsibilities and duties as a Trust. We only share information about you where it is **strictly necessary** for us to do so, and the law and our policies allow us to do this. The following are examples of who we share information with:

Department for Education (DfE)

We are required to share workforce information (this is known as the workforce census) with the DfE, so they can fulfil their statutory obligations relating to data collection. We are required to share information about our employees with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

To find out more about the data collection requirements placed on us by the DfE, including the data that we share with them, visit their website here

The DfE 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. For information about how the DfE collects and shares workforce data for research purposes, visit their website here

Our local authority

We are required to share information about our employees with our local authority under regulation 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments

Police and law enforcement agencies

We may be required to share information about any person we hold information about, to the police or other law enforcement agencies, to assist them in an investigation to prevent or detect a crime or safeguard individuals at risk.

Ofsted

We may be required to support an Ofsted inspection, where an inspector asks to see a sample of the Trust's records. These records could identify an employee. Any personal information the inspector may see, will not be taken away or used in their reports.

Schools within our Multi-Academy Trust

We may sometimes be required to share information about our employees within our Multi-Academy Trust (MAT), so we can monitor and assess the quality and consistency of our services across the MAT and provide shared resources. We will only share identifiable employee information, where this is strictly necessary to enable us to carry out a task in the public interest or our official duties as a Trust.

Service providers

We use companies that provide us with a service to help us run effectively as a Trust; the services we often receive are IT support, professional or legal advice, learning or teaching resources, communication services, catering or transport. To receive these services, we sometimes need to share personal information.

Our legal basis

The main legal bases we rely on when we process employee personal information are as follows:

- **It is necessary for us to perform a task which is in the public interest or to exercise our official duties as a Trust**
  This broad legal basis is applicable to almost all the processing we do involving personal data.
- **It is necessary for compliance with a legal obligation**

This is applicable where a specific law requires us to collect or share personal data This includes sharing data with the Department for Education (DfE), Her Majesty's Revenue and Customs (HMRC) and HM Courts and Tribunal Service.

- **It is necessary for the performance of a contract**
  This is applicable when we enter into a contract with you our employee.

- **The data subject has given their consent**
  Consent is not required for most of the processing we do, however, there are occasions when we ask for consent. For example, if we want to publish your photograph (headshot) on our website, social media or marketing material or collect your fingerprints to provide you with our cashless catering or library systems. Where we are processing your data with your consent, you have the right to withdraw that consent. If you change your mind, or if you are unhappy with our use of your personal data, please let us know by contacting the school office.

- **The processing is necessary to protect the vital interests of the data subject or someone else**
  This is applicable where a person's life could be at risk and we need to share or make available information to help them. This could involve sharing serious allergy information with other staff, paramedics (or other medical professionals), or other information requested by the police or social services, to assist them in their enquiries to protect that person.

When we process 'special category' data, we must have another legal basis. Special category data is personal data which reveals a person's racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data (such as fingerprints), health, sex life or sexual orientation. The main legal bases we rely on when we process this type of data is as follows:

- **The data subject has given explicit consent**
  This is usually applicable where we ask for health or dietary information.

- **The processing is necessary for performing any right or obligation which is imposed on the Trust in relation to employment, social security and social protection law (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud)**
  This is usually applicable where we are performing our duties under employment related laws e.g. in relation to health and safety, equality or tax or where we have taken action to safeguard individuals at risk.

- **It is necessary to protect the vital interests of any person where the data subject is physically or legally incapable of giving consent**

  This could be relied upon in situations where someone has become seriously ill on our premises and we are asked by medical practitioners (such as paramedics), to share information we know about that person's health or allergies.

- **The processing is necessary for the establishment, exercise or defence of legal claims**
  We may share or use special category data where legal action is being considered or underway.

- **The processing is necessary in the substantial public interest**
  This may be relied upon in circumstances where our processing is necessary to safeguard children or others at risk or where we respond to requests from the Police or law enforcement bodies, to assist in an investigation to prevent or detect an unlawful act.

- **The processing is necessary for the assessment of the working capacity of the employee**
  This will be applicable where an employee has been absent from work due to illness or injury and we need to assess whether they are fit to return to work.

This list is not exhaustive.

How we protect your information

We take our security responsibilities seriously in order to protect your personal data from accidental or unlawful access, disclosure, loss, damage or destruction. For example:

- Access to our data is on a strict need to know basis
- Our electronic records are held on encrypted servers
- We use up to date virus and malware protection software; security patches are applied promptly and we back up our data regularly
- Our sensitive paper files are locked away with restricted access to the keys
- Our employees, volunteers and governors are subject to Disclosure and Barring Service (DBS) checks and employee contracts contain confidentiality clauses
- We have policies, procedures and training around data protection, security, record disposal and confidentiality
- We have strict visitor management security procedures in place
- We use encrypted email or secure file sharing platforms to share personal data with external organisations
- We carry out due diligence checks on our service providers and Data Protection Impact Assessments, where required.

Storing personal data

The personal information we collect and store is essential for our Trust's operational use. We only keep personal information for as long as we need to, and where it is necessary to comply with any legal, contractual, accounting or reporting obligations. After this period, we delete or securely destroy personally identifiable data.

For more information about how long we keep personal data for, see our record retention schedule

Overseas transfers
We store our data in the UK or the European Economic Area (EEA), however some of our service providers may store personal data outside these areas (usually in the USA). We have a contract in place with these data processors, which ensures they process our data securely and in line with our data protection laws. To find out which service providers process data outside the EEA see **Our Service Providers.**

Your data protection rights

You have the following rights under the data protection laws:

Your right of access
You have the right to ask us for copies of your personal data. There are some exemptions, which means you may not always receive all the information we process.

Your right to rectification
You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure
You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing

You have the right to ask us to restrict the processing of your information in certain circumstances.

Your right to object to processing
You have the right to object to us processing your information where we consider this is necessary for us to perform a task in the public interest. You can also object to us using your contact details to send you direct marketing or fundraising communications, which you have previously opted-in to receiving.

Your right to data portability
This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another or give it to you. The right only applies if we are processing information based on your consent or under a contract (or in talks about entering into a contract) and the processing is automated.

Your right to complain
We work to high standards when it comes to processing your personal information. We hope you will always be happy with the way we handle your information, however if we have not met your expectations, please let us know so we can put things right. To do this, please email the Trust at cosec@ventrus.org.uk. If you remain dissatisfied, you have the right to complain to the Information Commissioner's Office (ICO). The ICO's contact details are available at https://ico.org.uk/concerns Further information about your data protection rights, can be found on the Information Commissioner's Office website at www.ico.org.

For information about how we handle requests from people exercising their rights, see our Data Protection Request Procedure available on our website.

Contact Us

There are many ways you can contact us, including by phone, email and post. Our contact details are as follows:

Ventrus Multi Academy Trust
Woodwater Academy
Woodwater Lane
Exeter
EX2 5AW

Email: Info@ventrus.org.uk
Telephone: 01392 256020

If you would like to make a request or complaint, please contact us. You are not required to pay a fee for exercising your rights and we have one month to respond to you.

Data Protection Officer
Our Data Protection Officer (DPO) is Amber Badley, an external consultant appointed under a service contract. If you have any queries about this privacy notice or any matter relating to the handling of your personal data, you can contact our DPO directly at DPO@firebirdltd.co.uk or by writing to the Trust at DPO@ventrus.org.uk

Changes to this privacy notice
We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated on 13 July 2020.