


PRIVACY NOTICE FOR STAFF

Status: Statutory

Updated: March 2023

Reviewed and ratified by: Audit, Risk and Resources Committee

Signed by Trust/Committee Chair



Next review date: March 2024

Published location: www.secat.co.uk



Southend East Community Academy Trust (SECAT) 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 work relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all current and former employees and workers.

Who collects this information?

SECAT is a 'Data Controller' for the purposes of data protection law. This means that we are responsible for deciding how we hold and use personal information about staff.

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and 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.

Personal data that we collect, process, hold and share

- Personal information and contact details such as name, title, addresses, date of birth, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including references, proof of right to work in the UK, application form, CV, qualifications;
- Employment contract information such as start dates, hours worked, post, roles;
- Education and training details;
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information on your sickness and absence records such as number of absences and reasons (including sensitive personal information regarding your physical and/or mental health);
- Your racial or ethnic origin;
- Criminal records information as required by law to enable you to work with children;
- Your trade union membership;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your timekeeping and attendance records;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Details of your use of business-related social media;
- Images of staff captured by the Trust's CCTV system;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the Trust, you will be notified separately if this is to occur); and
- Details in references about you that we give to others.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. We may collect this information from you, your personnel records, the Home Office, pension administrators, your doctors, from medical and occupational health professionals we engage, the DBS, your trade union, other employees, other professionals we may engage (eg. to advise us generally), automated monitoring of our websites and other technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities

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.

How we use your personal information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

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. Please note that we may process your information without your knowledge or consent, where this is required or permitted by law.

The situations in which we will process your personal information are listed below:

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employee's contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- To enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;
- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the Trust in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

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

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.

How we use particularly sensitive information

Sensitive personal information (as defined under the GDPR as 'special category data') require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to pension schemes);
- 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 necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

We will use this information in the following ways:

- Collecting information relating to leave of absence, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about your race or national or ethnic origin to ensure meaningful equal opportunity monitoring and reporting;
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. 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 or we may be notified of such information directly by you in the course of working for us.

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:

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

Who we share your information with

We may need to share your data with third parties, including third party service providers 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. These include the following:

- Department for Education (DfE);
- Ofsted;
- Other government departments or agencies;
- Prospective employers;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- Local Authority Designated Officer (LADO);
- Training providers;
- Professional advisors such as lawyers and consultants;

- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- Disclosure and Barring Service (DBS);
- Recruitment and supply agencies.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations; we require them to respect the security of your data and to treat it in accordance with the law.

Retention periods

Except as otherwise permitted or required by applicable law or regulation, the Trust only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the Trust considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether we can fulfil the purposes of processing by other means and any applicable legal requirements.

Once you are no longer an employee or worker of the Trust, we will retain and securely destroy your personal information in accordance with our data retention policy.

The Trust typically retains personal data for six years, subject to any exceptional circumstances, or to comply with laws or regulations that require a specific retention period.

Security

We have put in place measures to protect the security of your information (ie, against it being accidentally lost, used or accessed in an unauthorised way). 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.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

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.

The lawful basis on which we use this information

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life;
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and
- The Education Act 1996: for Departmental Censuses three times a year. More information can be found at: <https://www.gov.uk/education/data-collection-and-censuses-for-Trusts>.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

Your right of access to your personal data

Under data protection legislation, you have the right to:

- Access your personal information (commonly known as a 'subject access request'). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information;
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected;
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it;
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it;
- Object to processing in certain circumstances (for example for direct marketing purposes);
- Transfer your personal information to another party.

If you want to exercise any of the above rights, please email GDPR@secat.co.uk

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 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 email GDPR@secat.co.uk

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.

Contact us

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you email GDPR@secat.co.uk in the first instance to raise your concerns.

We have appointed a Data Protection Officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by emailing our internal Data Protection Lead TerryDignam@secat.co.uk then you can contact the DPO on the details below:

Data Protection Officer (DPO)

Name: Helen Wilson
Details: SBM Services
01206 671103
Email: helen.wilson@sbmservices.co.uk

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues at <https://ico.org.uk/concerns>.