



Job Applicant Privacy Policy

Recommended by Operations Director:	June 2026
Approved by Operations Committee:	June 2026
Review Due:	June 2027

Contents

Policy Statement	2
Definitions	2
Introduction	4
What Data does the Trust Process.....	4
During the application process	4
Pre-Employment.....	5
How we use your personal information	5
Use of your data for marketing purposes	5
Use of your data in automated decision-making and profiling	6
Use of your data for filtering and monitoring purposes.....	6
How long your data will be kept.....	6
Reasons we can collect and use your personal information	6
Our basis for using special category data	7
Collecting this data.....	8
Who do we share your personal information with	8
Transferring data internationally	9
Your Rights	9
Keeping your personal information secure	10
Complaints.....	10
Further information.....	10

1. Policy Statement

This notice explains what personal data (information) we hold about you, how we collect it, how we use it, and how we may share it. We are required to give you this information under data protection law.

2. Definitions

Term	Definition
Trust	is Marlow Education Trust, Sir William Borlase's Grammar Trust, West Street, Marlow, SL7 2BR

Term	Definition
Department of Education (DfE)	is the government department which deals with education
Local Authority (LA)	is Buckinghamshire County Council
Chair of Trustees	is Sarah Cooper
CEO	is Kevin Ford
Trust Headteacher	is registered on: https://get-information-trusts.service.gov.uk/
Trusts Data Protection Officer (DPO)	is Satswana Ltd, Suite G12 Ferneberga House, Alexandra Road, Farnborough, GU14 6DQ. admin@satswana.com
Data Protection Act (DPA)	The UK's primary data protection legislation. It sits alongside and supplements the UK GDPR, including UK-specific provisions, exemptions and enforcement arrangements.
UK General Data Protection Regulation (GDPR)	The UK's version of the GDPR, retained in domestic law. It sets out core data protection principles, rights and obligations, and is supplemented by the DPA 2018. The EU General Data Protection Regulation (EU GDPR) applies within the European Union.
Data (Use and Access) Act 2025 (DUAA)	Amends data protection, digital verification and smart data frameworks. Key education-sector changes include the ability to pause subject access request timescales during school holidays ('stop the clock'), a statutory reasonable and proportionate test for compliance with information rights, and the renaming of the Information Commissioner's Office (ICO) to the Information Commission (IC).
Freedom of Information Act (Fol)	The Freedom of Information Act 2000 discloses information held by public authorities or persons providing services for them and amends the Data Protection Act.
Educations Act (EA)	The Education Act 1996 consolidates the Education Act 1944 and certain other educational enactments.

Term	Definition
Information Commissioners Office (ICO)	The UK's independent regulator for data protection, freedom of information and related rights. It ensures compliance with the Data Protection Act, the Freedom of Information Act, and the UK GDPR, and handles formal complaints. (Formerly known as the Information Commissioner's Office (ICO); renamed under the Data (Use and Access) Act 2025.)
Electronic Platform	An electronic platform is any means the trust communicates. This could include, but is not limited to, Email, Online Portals, and Social Media platforms.

3. Introduction

Under UK data protection law, individuals have a right to be informed about how our 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 data.

This privacy notice explains how we collect, store and use personal data about individuals working with our trust or trust in a voluntary capacity, including governors. Our Trust is the 'Data Controller' for UK data protection law.

Our data protection officer is Satswana Ltd, also known as Trusts Data Protection Officer (DPO).

4. What Data does the Trust Process

As part of its operations, the Trust may process a wide range of personal data about individuals, including, by way of example:

a. During the application process

- Names, addresses, telephone numbers, email addresses, and other contact details.
- Personal details e.g. Date of Birth, National Insurance Number

b. Pre-Employment

- References given or received by the Trust and information provided by previous educational establishments, other professionals, or organisations working with pupils, or previous employers.
- Bank details and other financial information.
- Personnel data, such as Passports, Utility Bills, Driving Licenses, Birth Certificates, and Marriage Certificates, in connection with safeguarding, academic, and previous employment checks.
- Copies of right to work documentation.
- Evidence of qualifications
- Where appropriate, information about individuals' health, special needs, and contact details for their next of kin.
- Car Details (for those using our car parking facilities).
- Images of individuals engaging in trust activities and images captured by the Trust's CCTV system
- Visitor logs, login credentials, digital access, and other logs.
- Information about your use of our information and communication systems, equipment and facilities (e.g. trust computers).

5. How we use your personal information

We use your personal information to:

- Enable us to demonstrate relevant experience and qualifications.
- Facilitate safe recruitment as part of our safeguarding obligations pupils.
- Enable equality monitoring.
- Ensure that appropriate access arrangements can be provided for candidates who require them.
- Ensure that our information and communication systems, equipment, and facilities (e.g., trust computers) are utilised appropriately, legally and safely.

a. Use of your data for marketing purposes

Where you have given your consent, we may send you marketing information by email or text promoting trust events, campaigns, charitable causes, or services that may interest you. You can withdraw consent or 'opt out' of receiving these emails or texts at any time by clicking on the 'Unsubscribe' link at the bottom of any such communication or by contacting the Trust.

b. Use of your data in automated decision-making and profiling

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

c. Use of your data for filtering and monitoring purposes

While in our Trust, we may monitor your use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so that we can:

- Comply with health and safety and other legal obligations.
- Comply with our policies (e.g. child protection policy, IT acceptable use policy) and our legal obligations.
- Keep our network(s) and devices safe from unauthorised access and prevent malicious software from harming our network(s).

6. How long your data will be kept

We will retain personal data only for as long as necessary for the purposes for which it was collected or as required by law. We have implemented a data retention policy which sets out the retention periods for different categories of personal data. For example:

- Job Applicants: If your employment application is unsuccessful, the Trust will hold your data on file for six months after the end of the relevant recruitment process (in line with the Equality Act 2010 limitation period for employment tribunal claims). Under the Data (Use and Access) Act 2025, subject access request timescales may be paused during school holiday periods ('stop the clock' provision).
- Successful applicants, we will store your data for as long as you are an employee, and for seven years after your employment ends.
- CCTV footage: retained for up to 30 days unless required for an investigation.

We will take reasonable steps to securely delete or anonymise personal data when it is no longer needed.

7. Reasons we can collect and use your personal information

We collect and use your personal information to fulfil our legal obligations and perform tasks that serve the public interest. We rely on the following legal bases under the UK GDPR:

- Article (6)(1)(b) - Contractual necessity: the processing is necessary for performing or entering into a contract with you (including pre-contractual steps taken at your request).
- Article (6)(1)(c) - Legal obligation: the processing is necessary to comply with the law.
- Article (6)(1)(e) - Public task: the processing is necessary to perform a task in the public interest or for official functions (task or function has a clear basis in law).

When we collect or share 'special category' personal data, we rely on the following legal bases under the UK GDPR:

- Article 9(2)(g) - Reasons of substantial public interest
We rely on the Equality of opportunity or treatment purpose condition from Schedule 1 of the Data Protection Act 2018 when relying on Article 9(2)(g) to process your special category data.
- Article 9(2)(h) - Health or social care (if a case needs to be stepped up to children's social work services or the management of social care systems or services)
- Article 9(2)(j) - Archiving, research and statistics (for scientific or historical research purposes or statistical purposes)
- Article 9(2)(f) - Legal claims or judicial acts (for the establishment, exercise or defence of legal claims whenever courts are acting in their judicial capacity).

a. Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your data in a specific manner.
- We need to fulfil an obligation or exercise a right concerning employment, social security, or social protection law.
- We need to protect an individual's vital interests (i.e., protect your life or someone else's life) in situations where you are physically or legally incapable of giving consent.
- The data in question has already been made manifestly public by you.
- We need to process it for the establishment, exercise, or defence of legal claims.
- We need to process it due to substantial public interest as defined in legislation.
- We need to process it for health or social care purposes, and the processing is carried out by, or under the direction of, a health or social work professional or by any other person required to maintain confidentiality under law.
- We need to process it for public health reasons, and the processing is conducted by, or under the direction of, a health professional or by anyone bound to confidentiality under law.
- We need to process it for archiving, scientific or historical research, or statistical purposes, and the processing is in the public domain interest.

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

- We need to fulfil an obligation or exercise a right concerning employment, social security, or social protection law.
- We have obtained your consent to use it for a specific purpose way.
- We need to protect an individual's vital interests (i.e., protect your life or someone else's life) in situations where you're physically or legally incapable of giving consent.
- The data in question has already been made manifestly public by you.

- We need to process it for legal proceedings, to obtain legal advice, or for establishing, exercising, or defending legal rights.
- We need to process it due to substantial public interest as defined in legislation.

8. Collecting this data

While most of the information we collect about you is mandatory, some information can be provided voluntarily.

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

Most of the data we have about you will come from you, but we may also possess data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals

When data is received from a third party, we are not the controllers of the data and would need to obtain permission to share it. The data controller can legitimately refuse your request.

9. Who do we share your personal information with

We do not share information about you with any third party without your consent, unless required by law or our policies.

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

- DfE, other government agencies and local authorities as required (e.g. to resolve rights to work or the Teaching Regulation Agency (TRA) which maintains the list of teachers prohibited from teaching).
- LA teams are working to improve outcomes for children and young people.
- Commissioned providers of LA services (such as education services).
- Other trusts or colleges that you may work at after leaving us.
- Our LA to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as HR and recruitment support, and filtering and monitoring IT use.
- Professional advisers and consultants
- Employment and recruitment agencies.

We will share personal information with law enforcement or other authorities if required by applicable law.

a. Transferring data internationally

We may share personal information about you with the following international third parties, where different data protection legislation applies:

- Other trusts or educational establishments
- Government departments or agencies
- Security organisations

We will transfer data based on an adequacy regulation (previously referred to as an 'adequacy decision') issued by the UK government.

When we transfer your data to a third-party country or territory, we will do so in accordance with UK data protection law.

In cases where we need to establish safeguarding arrangements to complete this transfer, you can obtain a copy of these arrangements by contacting us.

10. Your Rights

Under the UK GDPR, you have rights which you can exercise free of charge, which allow you to:

- Know what we are doing with your information and why we are doing it.
- Ask what information we hold about you (Subject Access Requests).
- Ask us to correct any mistakes in our information about you.
- Object to direct marketing.
- Make a complaint to the Information Commission (IC).
- Withdraw consent (if applicable).

Depending on our reason for using your information, you may also be entitled to:

- Ask us to delete the information we hold about you.
- Have your information transferred electronically to yourself or another organisation.
- Object to decisions being made that significantly affect you.
- Object to how we are using your information.
- Stop using your information in specific ways.

We will always seek to comply with your request. However, we may be required to hold or use your information to comply with legal duties. Please note: your request may delay or prevent us from delivering your service.

For further information about your rights, including the circumstances they apply, see the ICO's guidance on individuals' rights under GDPR.

If you would like to exercise a right, please get in touch with our DPO.

11. Keeping your personal information secure

We take the security of personal data seriously and have implemented appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and accidental loss, destruction, or damage. These measures include:

- Regular data protection training for staff
- Use of strong passwords and encryption
- Regular security assessments and audits
- Secure storage and disposal of personal data
- Restriction of access to personal data to authorised personnel only

In the event of a data breach, we will take appropriate steps to mitigate the impact and comply with our legal obligations, including notifying affected individuals and the Information Commission (IC) where necessary.

12. Complaints

If you have any concerns about how we handle your data, please don't hesitate to contact our Data Protection Officer (DPO). If you are unsatisfied with our response, you can complain to the Information Commissioner's Office (ICO).

You can contact the ICO at:

Information Commission Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF

Tel: 0303 123 1113

Report a concern online at <https://ico.org.uk/make-a-complaint/>

13. Further information

For further information about how the DfE uses your information:

For more information about the DfE's data-sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>.

To contact DfE: <https://www.gov.uk/contact-dfe>