Somerset Road Education Trust

Privacy Policy

Version and Date		Action/Notes
1.0	23/5/2018	Approved by SRET

Somerset Road Education Trust

Table of Contents

Introduction

Somerset Road Education Trust (SRET), as an educational establishment, needs to collect and use information on individuals such as pupils, parents, guardians, trustees, governors, staff members and visitors. We use this information to manage the school and meet our legislative requirements. However, we must ensure that we use and protect the information in accordance with current legislation. Failure to do so could lead to distress to individuals, reputational damage and financial sanctions from the Information Commissioner's Office (ICO).

This policy, together with other documents (Funding Agreement, Articles of Association, Retention Policy and Privacy Notices) describes how we will protect personal information to protect the individual and comply with the law.

Definitions

Data Controller

SRET, Exeter House School, St Mark's C of E Junior School and Wyndham Park Infants School are the data controllers and are registered with the ICO, we are responsible for all the personal information we collect.

Data Subject

The data subjects are the individuals whose personal information we deal with, such as pupils, parents, guardians, trustees, governors, staff members and visitors.

Personal Information

Personal information means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, from the information. The information includes name, address, date of birth, email, telephone number, national insurance number, payroll number and online identifier such as a username. Personal information also includes information associated with that individual such as school marks, exam results, special educational needs assessments, staff development, staff reviews and pay rates.

Sensitive information such as medical, race, religion, sexuality, political or trade union membership are a special category of data that requires sensitive handling.

Data Processing

Processing means any action performed on personal information, which includes collection, recording, organising, storing, sharing and transmitting. This includes electronic and paper documents containing personal information. Many of the activities within the school involves processing information and therefore we must comply with the law.

Legislation

The schools must comply with the Data Protection Act (DPA) and the EU General Data Protection Regulation (GDPR).

Governance

Roles and Responsibility

Everyone associated with Somerset Road Education Trust has a responsibility to ensure we protect the personal information we hold and comply with this policy.

Board Level

Trevor Branch, Trustee, is accountable to the SRET Board of Trustees for data privacy and will report to the board on data privacy every quarter.

Data Protection Officer

AJ Security Consultancy Ltd is the Data Protection Officer (DPO) and has day-to-day responsibility for data privacy, they are the main point of contact for any questions about data privacy. Email Contact: info@ajsecurityconsulting.co.uk

Staff/Trustee Responsibilities

All staff and Trustees are responsible for complying with this policy.

Reporting

The DPO will produce a quarterly report on data privacy for the Trust Board.

Risk Management

Data Privacy Impact Assessment (DPIA)

When we are considering processing information in new way or using a new technology, such as hosting personal information in the cloud or using a mobile phone application to record pupil progress, the DPO will decide whether a Data Privacy Impact Assessment (DPIA) is required.

Risk Summary Document

The DPO will maintain a risk register of the school's data protection risks. The register will be reviewed annually by the Trust Board.

Privacy Principles

Collecting Information

We should collect the minimum information we need to complete a task. **We should not collect information just in case.**

Processing Information

When we are planning to process information, we must consider whether we need the individual's consent to process. The majority of our processing is for legitimate business reasons to run our school; we need to pay staff, monitor and report on pupil progress and therefore we do not require consent. However, some activities may not be considered school business, such as making charity appeals, advertising services not related to the school or sharing parent information with a parent association. We must obtain and record consent for this processing. We must store this consent and review it every three years.

Securing Information

We must protect the personal information we use whether in electronic or paper format:

- Documents containing personal information should be stored in a secure cabinet or container when not required.
- Documents containing pupil, parent or staff information should only be removed from school premises where necessary. Documents must be protected while off school premises and should not be left unattended.
- Electronic copies of personal information must be stored on a Somerset Road Education Trust controlled device.
- When a device containing personal information leaves the school premises, the personal information should be protected by encryption.
- Electronic documents containing pupil, parent or staff information should not be emailed to staff home computers or personal mobile devices.
- Staff should not download electronic documents containing pupil, parent or staff information on their own devices.

Data Retention

When personal information is no longer required and there is no legal requirement to retain the information. Electronic data must be deleted and paper copies securely destroyed. Our Retention Policy contains a list of how long we need to retain the types of information we process.

Subject Access Request and Data Transfer Request

Individuals have the right to know whether we store and process their personal information, this is known as a Subject Access Request. If the information we hold is inaccurate they have the right for that information to be corrected. In certain circumstances, they have the right to have the information deleted or to be given a copy of that information. We have to respond to any request within one month. The individual does not have to state they are making a subject access request, it can be a simple email asking what information we hold, and therefore, any request by an individual with regards to the information we hold must be forwarded to the DPO who will advise the Headteacher on how to respond. Only the Headteacher can authorise the release of personal information.

Individuals have a right to make a "subject access request" to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been or will be shared with.
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period.
- The source of the data, if not the individual.

- Whether any automated decision-making is being applied to their data and what the significance and consequences of this might be for the individual.

Children and subject access requests

The ICO state that even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong, for example, to a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, the DPO will consider whether the child is mature enough to understand their rights. If there is confidence that the child can understand their rights, then the DPO will respond to the child rather than a parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, the following will be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, the law presumes that a child aged 12 years or more has the capacity to make a subject access request. The presumption does not apply in England and Wales or in Northern Ireland, but it does indicate an approach that will be reasonable in many cases. It does not follow that, just because a child has capacity to make a subject access request, they also have capacity to consent to sharing their personal data with others – as they may still not fully understand the implications of doing so. The DPO will therefore consider each request on an individual basis.

Communication

Somerset Road Education Trust is registered with the ICO as a data controller and data processor. The SRET Business Manager is responsible for maintaining our registration.

We will have a privacy notice which will clearly inform individuals how we collect their information, what we do with their information and their rights. A copy of the privacy notice

will be displayed prominently on our website and a copy will be sent to individuals when we are requesting information from them.

The DPO is responsible for maintaining the privacy notice.

Education and Awareness

All new joiners, including temporary staff, must read this privacy policy as part of their induction process.

All staff will receive annual data privacy training as part of their ongoing staff development.

The DPO will periodically send emails to all staff highlighting key aspects of data privacy.

Incident Handling

We have a legal responsibility to report certain data privacy incidents to the ICO within 72 hours or face a financial penalty. It is essential that all staff follow the incident procedure. Example of privacy breaches are:

- Emailing a child's medical information to a wrong parent or guardian.
- Leaving a bag containing several children's annual assessments in Waitrose cafe.
- Losing a laptop or mobile device containing the personal information of a large number of pupils and staff.

Not all the examples above are reportable to ICO however it is essential that staff report any incident or potential incident to the DPO. The DPO will then discuss with the Headteacher and accountable Trustee and decide whether the incident requires reporting to the ICO and whether an action is required to manage the risks from the incident.

Assurance and compliance

The DPO will carry out periodic checks to monitor staff compliance with this policy.

Steve De Bruin of Bath & Somerset Council will carry out annual checks on our compliance.

Policy Reviewed:	May 2018
Next Review:	
Signature of Chair of Trustees	Signature of Executive Principal