SHERBORNE AREA SCHOOLS' TRUST

Data Protection Policy

Published:	**25 May 2018**
Review due:	**June 2019**
Author:	**DPO**

SAST Schools' Data Protection Policy

2017-2018

Sherborne Area Schools' Trust understands its legal obligations in protecting the privacy of staff and pupils through strict control, management and security of personal data. As part of its operation, the Trust and SAST Schools collect confidential and personal data from pupils, parents, and staff and processes it in order to support teaching and learning and wider operation of the Trust and schools.

Under the General Data Protection Regulations 2018 (GDPR) any data we have recorded whether in paper or digital form can only be used in accordance with six strict principles. It must be:

1. processed fairly and lawfully
2. only be obtained for one or more specified and lawful purposes in a way that is adequate, relevant and not excessive
3. adequate, relevant and not excessive in relation to the purpose or purposes
4. accurate and kept up to date
5. kept for no longer than is absolutely necessary, and,
6. processed only in accordance with the rights of the "Data Subject"

1. We Promise to Keep Data Safe

We take responsibility for ensuring that any data that we collect and process is kept securely and used lawfully. SAST schools and The Trust will keep pupils, staff and parents/carers fully informed of how data is collected, what is collected, and how it is used. Contact details, academic results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that schools' need. Through effective data management we can monitor and evaluate the wellbeing and academic or professional development of all our pupils and staff to ensure that we are doing all that we can to support them. A Privacy Notice is issued to Data Subjects when they join the Trust so they are aware of the personal data we keep secure and how SAST schools and the Trust may use it.

2. Your Right to Access Your Data

When a pupil or staff member joins the Trust we ask that pupil and/or their parent/carers or in the case of staff, the staff member themselves to provide us with personal data. That data is not owned by SAST and remains the property of that pupil, their parent/carer or staff member, respectively. Under GDPR, the person who owns the data is called the "Data Subject". The Data Subject is the person who owns the personal information because it is about them. As a Data Subject, adults and children over 13 years (or their parent/carer with parental responsibility) has the following rights which SAST must recognise and uphold:

- a right of access to a copy of the information comprised in their personal data
- a right to object to processing that is likely to cause or is causing damage or distress

- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means (decisions taken by software rather than staff)
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed, and,
- a right to claim compensation for damages caused by a breach of the Regulations.

If a "Data Subject" wishes to use their right to see a copy of the data SAST holds, they or their parent/carer should write to SAST's Data Protection Officer asking to make a "Subject Access Request" (SAR) under GDPR. You can do this by email to DPO@sast.org.uk or by letter to:

The Data Protection Officer
Sherborne Area Schools' Trust
c/o The Gryphon School
Bristol Road
Sherborne DT9 4EQ

Making a SAR is free and you can expect a response within 30 days. In a SAR, the Data Subject has the right to ask some very specific questions about his/her data including:

- confirmation that SAST are processing your personal data;
- a copy of your personal data;
- the purposes that SAST processes for;
- the recipients or categories of recipient SAST shares the personal data with;
- how long SAST will retain or store the personal data;
- asking for any errors to be corrected
- asking for data to be erased or to restrict or object to some or all of the data being stored/processed;
- where the information being processed about you came from if it was not provided by you directly;
- whether any of your data is processed using software which uses automated decision-making or profiling tools;
- where SAST uses Cloud storage, that the actual location of the data (if outside the EU, in the US for example) is transferred to the data host safely.

If a Data Subject feels something is amiss in the way SAST processes their data, the DPO can be notified of the problem directly. The DPO will then liaise with staff to ensure everything is in order. Where a problem cannot be resolved easily, and they otherwise have a right to lodge a complaint with the Information Commissioners Office (ICO), the UK data processing supervisory authority. Contact details for ICO can be found at www.ico.org.uk/concerns.

3. How We Secure Your Data

The Data Protection Officer advises SAST school staff and the Trust about meeting strict rules around keeping data safe. There are several ways this is achieved:

1. Data security audits are carried out regularly
2. Data Protection Impact Assessments are made on data held in all of our systems so we are fully aware of the likelihood and impact on Data Subjects in the event data privacy is compromised.
3. Digital software systems and paper filing systems in which personal are stored are secured with physical barriers such as locks and permission restrictions and/or software that restricts who can view it, detects data transfer, prevents damage from viruses or malware.
4. For especially private data additional security measures such as encryption or anonymisation are also used.
5. All staff receive regular training and have to follow procedures to ensure data security which is regularly monitored.

SAST staff have restricted access to pupil or staff personal data and are only given access on a 'need to know' basis in the course of their duties within SAST. Staff are only permitted to use data for the purpose for which it was collected, and any staff that are found to be acting intentionally in breach of GDPR or any Trust data use or security policy will be disciplined in line with the seriousness of their misconduct.

4. Sharing Personal Data with Third Parties

There are circumstances where a SAST school is required to share personal data it holds with other parties in order to perform its public duty. The data shared with third parties is strictly limited to only that data which the third party needs to fulfil its contract. The third parties working with SAST schools include, among others; PTFAs, after school clubs, school milk providers, special skills teachers, Dorset County Payroll and HR services, IT support, exam providers, school meals providers, school photographer etc. Every third party must sign a Data Processing Agreement and verify that they are compliant with the General Data Protection Regulation without which no sharing is allowed. The verification process is thorough and carefully managed.

SAST schools or the Trust may also be required by law or in the best interests of our pupils or staff to pass information onto external authorities, for example to Dorset County Council, Ofsted, the Department of Health or the Police. These authorities must also comply with GDPR.

Under no circumstances will SAST disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of SAST or local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption

from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

5. Sharing Data and Consent

For the majority of purposes listed above where SAST schools or the Trust is sharing data with third parties, consent from the Data Subject is not required, so long as, the data is being processed lawfully (in the course of its public duty, under contract, because of a legal obligation, as a legitimate interest of the school or Trust or to protect the vital (health and welfare) interests of the pupil or staff member). However, there are some circumstances where consent must be obtained from a Data Subject prior to SAST schools or the Trust processing the data. These circumstances include using a photograph or video for marketing purposes and collecting biometric data for pupils or staff to access photocopiers or canteen payment systems (some SAST schools only).

6. Privacy Notices

SAST will issue a Privacy notice to all pupils and staff when they join the Trust. SAST will not collect or process any biometric data of any pupil without parental consent. This includes fingerprint identification and also covers iris and retina scanning, and face recognition. SAST will not collect or process any photographic or video data without consent. If SAST wishes to collect either photographic, video or biometric data, pupils over 13 or parents/carers or staff (as appropriate) will be contacted for consent. This request for consent will include full explanation about the type of information that will be taken and how it will be used, as well as an explanation of the staff member, parents' and/or pupil's right to refuse or withdraw their consent.

7. Security in Practice

Records and personal information in paper form will be stored out of sight and in a locked cupboard no matter what format it is in. The only exception to this is medical information that may require immediate access during the school day. This will be stored either in the SAST School offices or the SEND offices.

Sensitive or personal information and data will not be removed from SAST school sites except where necessary. SAST acknowledges that some staff may need to transport data between SAST school premises and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils. The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off SAST school sites except where securely stored in a lockable bag or case. No information should be on view in public places, or left unattended under any circumstances.
- Paper documents will not be left on a desk unattended during the day and must be filed away overnight in a locked cupboard.
- Unwanted paper copies of data, sensitive information or pupil files will be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to access data away from SAST school premises, it can be viewed via remote access to the IT network or via encrypted email. USB sticks are not permitted unless secured with a pin code or password protection system. No data may not be transferred from a portable storage device onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

These guidelines are clearly communicated to all SAST staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.