

TSS Data Protection and Freedom of Information Policy 2025

Date Accepted:	July 2025
Review Date:	July 2026

1 Policy Statement

We must protect the data and information we hold on any individual and will do so under the guidance of the law.

2 Definitions

Term	Definition
School	is Trinity St Stephen Church of England First School, Vansittart Road, Windsor SL4 5DF
Department of Education (DfE)	is the government department which deals with education
Local Authority	is Royal Borough of Windsor and Maidenhead
Headteacher	is Louise Lovegrove
Chair of Governors (CoG)	is Trevor Kirby
Business Manager	is Kim Jones
Designated Safeguarding Leads (DSL)	is Louise Lovegrove
Schools Data Protection Officer (DPO)	is Satswana Ltd, Suite G12 Ferneberga House, Alexandra Road, Farnborough, GU14 6DQ. info@satswana.com
Data Protection Act (DPA)	The Data Protection Act 2018 makes a provision about the processing of personal data, which is subject to GDPR, with an amendment in 2023.
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.
UK General Data Protection Regulation (GDPR)	which applies across the European Union (including in the United Kingdom)
Educations Act (EA)	The Education Act 1996 consolidates the Education Act 1944 and certain other educational enactments.
Information Commissioners Office (ICO)	This organisation ensures compliance with the Data Protection Act, Freedom of Information Act, and GDPR and handles formal complaints.
Electronic Platform	An electronic platform is any means the school communicates. This could include, but is not limited to, Email, Online Portals, and Social Media platforms.

Term	Definition
Sensitivity Labels	<p>Are labels applied to electronic documents to support data protection within the school? The following labels are active:</p> <ul style="list-style-type: none"> • Highly Confidential – Do not leave the site. • Confidential – Can leave the site but must be encrypted. • General – Can leave the site. • Personal – Discretion of the end user. • Public – Is available to the public.

3 Aims & Objectives:

This policy aims to provide a model set of guidelines to enable staff, parents, and children to understand:

- The law regarding personal data.
- How personal data should be processed, stored, archived, and deleted/destroyed.
- How staff, parents and children can access personal data.

In addition, there is brief guidance at the end of the policy on FoI, which covers other information held by schools.

The policy's objective is to ensure that the school acts within the requirements of the DPA when retaining and storing personal data and making it available to individuals and that responding to enquiries for other information is also legal under the FoI.

3.1 Data Protection

Under the DPA and other regulating acts, access to their personal information is a statutory right for children (if they are of an age to understand the information they request), and parents (as defined in the EA) may also request access to their child's data.

School staff have a right of access to personal data on themselves.

Anyone has the right to question and correct inaccurate information, but this must be matters of fact, not opinions.

Personal data should always be kept securely and protected by passwords if it is electronic, and access to it should only be by those authorised to see it – confidentiality should be respected. The law also states that personal data should not be kept longer than required.

Third-party data (information about someone other than the requesting individual) should only be provided with their permission.

It is the responsibility of all staff in the school to follow this policy; the School's DPO provides guidance and compliance for all data held by the school.

The Headteacher is accountable for all personal data held by the school and will provide the right level of monitoring and scrutiny.

4 Guidance in processing, storing, archiving and deleting personal data

- Through the application process, a new staff member can request sensitive documentation, e.g., a passport or birth certificate. Once these checks are complete, they need to be destroyed.
- Children's admission – The admin team will view the verification document, either birth certificate or passport, but will not copy the document.
- Personal data and school records about children are confidential to the child. The information can be shared appropriately within the school's professional work to enable the school to provide the child with the best educational provision. The law permits such information to be shared with The DfE for census and other educational establishments only when a pupil changes schools.
- School records for a child should be kept for seven years after the child leaves the school or until the child reaches 25 years of age (whichever is greater), and examination records should be the same. School always transfers all

child records to the next school. In the event of the child leaving the country, the records would be held at the School.

- Data on staff is sensitive information and confidential to the individual. It is shared, where appropriate, at the discretion of the Headteacher and with the knowledge and, if possible, the agreement of the staff member concerned.
- Employment records form part of a staff member's permanent record. Because specific legislative issues are connected with these (salary and pension details, etc.), these records should be retained as set out by the Local Authority.
- When an employee leaves the School, their information is retained for seven years.
- Interview records, CVs and application forms for unsuccessful applicants are kept for six months after the interview.
- All Financial information is held for seven years.
- The school may collect and share further data on staff not covered by the above. This could be, for example, for Continuous Personal Development (CPD), celebration, promotion, etc. and may be in digital or non-digital format. The processing, storing, accessing, archiving, and deleting of such data will be agreed upon with the staff members involved on a case-by-case basis.
- All formal complaints made to the Headteacher or CoG will be kept in confidential files for at least seven years, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and legal professional privilege in the event of a court case.

5 Guidance on accessing personal data

- A child can request access to his/her data. The request is not charged and does not have to be in writing. The staff will judge whether the request is in the child's best interests and that the child will understand the information provided. They may also wish to consider whether the request has been made under coercion.
- A parent can request access to or a copy of their child's school records and other information about their child. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be a charge for photocopying records detailed in guidance from the ICO. Staff should check if a parent requests information and that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force.
- Parents should note that all rights under the DPA to do with information about their child rest with the child as soon as they are old enough to understand these rights. This will vary from child to child, but as a broad guide, it is reckoned that most children will have a sufficient understanding by 12. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.
- Separately from the DPA, The Education (Pupil Information) (England) Regulations 2005 provide a child's parent (regardless of the age of the pupil) with the right to view or to have a copy of their child's educational record at the school. Parents who wish to exercise this right must apply to the school in writing.
- For educational records (unlike other personal data; see below), access must be provided within 15 school days, and if copies are requested, these must be supplied within 15 school days of payment.
- A staff member can request access to their records at no charge, but the request must be made in writing. The staff member can see their records and ask for document copies. There is no charge for copies of records.
- The law requires that all requests for personal information are dealt with within 40 days of receipt except requests for educational records (see above). All requests will be acknowledged in writing on receipt, and access to records will be arranged as soon as possible. If awaiting third-party consent, the school will arrange access to those already available documents and notify the individual that other documents may be available later.
- In all cases, should third-party information (information about another individual) be included in the information, the staff will try to obtain permission to show this information to the applicant, except for information provided by another member of the school staff (or Local Authority) which is exempt from a requirement for third party consents. If third-party permission is not obtained, the person responsible should consider whether the information can still be released.
- Personal data should always be directly relevant to the person requesting the information. A document discussing more general concerns may not be defined as personal data.

- The FoI came into force, a request for personal information can include unstructured and structured records – for example, letters, emails, etc., not kept within an individual's files or filed by their name but still directly relevant to them.
- Anyone who requests to see their data has the right to question the accuracy of matters of fact within the data and to ask for inaccurate information to be deleted or changed. They may also question opinions, and their comments will be recorded, but opinions do not need to be deleted or changed as a part of this process.
- The school will document all requests for personal information with details of who handled the request, what information was provided and when, and any outcomes (letter requesting changes, etc.) This will enable staff to deal with a complaint if one is made concerning the request.

6 Fair processing of personal data

The School, Local Authority and the DfE all hold information on children to run the education system, and in doing so they have to follow the DPA. This means, among other things, that the data about children must only be used for specific purposes allowed by law. The school has a Fair Processing or Privacy Notice, which explains how personal data is used and with whom it will be shared. This Notice is published on the school website.

- The School, LA, the DfE, Agency and Ofsted all process information on children in order to run the education system, and in doing so have to comply with the DPA. This means, among other things, that the data held about children must only be used for specific purposes allowed by law. We are therefore writing to tell you about the types of data held, why that data is held, and to whom it may be passed on.
- The school holds information on children in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing. This information includes contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information. From time-to-time schools are required to pass some of this data to Local Authority's, the DfE and agencies, such as the Teaching Agency and Ofsted, that are prescribed by law.
- The Local Authority uses information about children to carry out specific functions for which it is responsible, such as assessing any special educational needs the pupil may have, pupil tracking, etc. It also uses the information to derive statistics to inform decisions on, for example, the funding of schools, to assess the performance of schools, and for target-setting purposes. The statistics are used in such a way that individual children cannot be identified from them.
- The Teaching Agency uses information about children to administer the National Curriculum tests and assessments for any key stage. The results of these are passed on to the DfE in order for it to compile statistics on trends and patterns in levels of achievement. The Teaching Agency uses the information to evaluate the effectiveness of the National Curriculum and the associated assessment arrangements, and to ensure that these are continually improved. This information may be shared with other Government departments or agencies strictly for statistical or research purposes only.
- OfSTED uses information about the progress and performance of children to help inspectors evaluate the work of schools, to assist schools in their self-evaluation, and as part of Ofsted's assessment of the effectiveness of education initiatives and policy. Inspection reports do not identify individual children.
- The DfE uses information about children for research and statistical purposes to inform, influence, and improve education policy and monitor the performance of education services. The DfE will feed back to Local Authority and school information about their children for various purposes, including data checking exercises, use in self-evaluation analyses and where information is missing because a former school did not pass it on. The DfE will also provide Ofsted with child-level data for school inspection.
- Child information may be matched with other data sources that the DfE holds to model and monitor children's educational progression and provide comprehensive information to Local Authority's and learning institutions to support their day-to-day business. The DfE may also use contact details from these sources to obtain samples for statistical surveys. These surveys may be carried out by research agencies working under contract with the DfE, and participation in such surveys is usually voluntary. The DfE may also match data from these sources to data obtained from statistical surveys.
- Child data may also be shared with other Government Departments and Agencies (including the Office for National Statistics) for statistical or research purposes only. In all these cases the matching will require that individualised data is used in the processing operation, but that data will not be processed in such a way that it supports

measures or decisions relating to particular individuals or identifies individuals in any results. The Department's Chief Statistician will approve and control this data sharing.

- Children, as data subjects, have certain rights under the DPA, including a general right of access to personal data held on them, with parents exercising this right on their behalf if they are too young to do so themselves. If you wish to access the personal data held about your child, then please get in touch with the school.

7 Publication Schemes

Under the FoI, the school has a publication scheme, a formal list of the types of non-personal information which the school produces or holds, and which is readily accessible to staff, children parents or other enquirers, as follows:

The scheme covers information already published and information that is to be published in the future. All information in our publication scheme is available on paper. Some information we hold may not be public, e.g., personal information. This publication scheme conforms to the model scheme for schools approved by the ICO.

7.1 Categories of information published:

- School Brochure.
- Governor Minutes, when the school has a Full Governing Body.
- School Profile.
- School Policies and other information related to the school.
- Data Protection.
- Freedom of Information Notices to children.
- Newsletter.
- Website.
- Parent mail.
- Texting.

7.2 How to request information:

Contact the School stating publication required and your name.

7.3 Paying for information:

All documents are available to view in the school office. Copies may be requested; a charge will be levied to cover the photocopying cost.

Classes of Information Currently Published

- Information required by Statute.
- School Brochure.
- School Profile.
- School Policies.
- Minutes of the Governing Body*

*Some information might be confidential or otherwise exempt from publication by law - we cannot, therefore, publish this.

7.4 Policies and policy statements

A complete list is published on the website.

7.5 Mental Health and Wellbeing

The school has an established culture that promotes and enhances the positive mental health of the whole school community. We recognise that healthy relationships underpin positive mental health and have a significant impact on learning, health, and well-being. We champion the expectation that 'mental health is the individual's responsibility supported by the whole school community.'

7.6 Feedback and Complaints:

Comments and suggestions are welcome. Please address this to the CoG at the School.

If you are not satisfied with the response from the CoG, please get in touch with the ICO.

8 Requests for information

- All schools which receive a written or emailed request for information which they hold or publish, are required to respond within 20 working days.
- A refusal of any information requested must state the relevant exemption which has been applied or that the school does not hold the information and must explain what public interest test has made if this applies.
- If the information is published by another organisation (for example, Ofsted reports) the school can direct the enquirer to the organisation which supplied the information or publication unless it is legal and possible to provide the information direct (for example, a copy of the summary of an Ofsted report).
- It will not be legal to photocopy a publication in its entirety and supply this to an enquirer unless the school owns the copyright.
- The school will keep the original request and note against this who dealt with the request and when the information was provided.
- Any complaint about the provision of information will be handled by the Headteacher. All complaints should be in writing and documented. The Publication Scheme will include information on who to contact for both enquiries and complaints.
- All enquirers should be advised that they may complain to the ICO if they are unhappy with the way their request has been handled.

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

If a staff member, governor, or data processor finds or causes a breach or potential breach, they must immediately notify the DPO.

- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been.
 - Made available to unauthorised people.
 - Made unavailable, with a significant adverse effect on individuals.
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or is likely to occur, the DPO will alert the Headteacher and the CoG.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers.)

- The DPO will assess the potential consequences based on how serious they are and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO, or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the '[report a breach](#)' page of the ICO website within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach, including, where possible:
 - The categories and approximate number of individuals concerned.
 - The categories and approximate number of personal data records concerned.
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain why there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
 - Any clear and specific advice on how the individuals can protect themselves and what the school is willing to do to help them.
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts, including the cause.
 - Effects
 - Action taken to contain it and make sure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored in the School's IT Infrastructure. The DPO and Headteacher We will meet as soon as reasonably possible to review what happened and how it can be prevented from happening again.
- The DPO and Headteacher will meet as part of the Senior Leadership Team (SLT) termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

8.1 Actions to minimise the impact of data breaches.

Below, we set out the steps we might take to mitigate the impact of different types of data breaches if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- Where at all possible, electronic data will be labelled in accordance with the Sensitivity Labels:

- If data is made public, it must be the final version and approved by the Headteacher and the CoG.
- Where possible the IT system will be configured to ensure that data is properly secured.
 - But in the event of sensitive information accidentally made available to unauthorised individuals via an electronic platform, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
 - If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
 - In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the DSL and discuss whether the school should inform any, or all, of its safeguarding partners.