



**ST IVO SCHOOL**  
**Data Policy**

**Incorporating General Data Protection Regulation and Freedom of Information**

Approved: January 2019, Governors Staff and Student Committee

Next review due: January 2020

**1. Scope and Purpose of this Policy**

- 1.1 This policy applies to all staff and governors in the handling of data on behalf of and for St Ivo School
- 1.2 This policy will be reviewed every two years by the Governing Body (Personnel Committee)
- 1.3 Readers of this policy may also wish to refer to the school's ICT policy

**2. Roles & Responsibilities**

- 2.1 The school has a Data Protection and Freedom of Information Officer appointed by the Headteacher. He/she is responsible for:
  - reviewing this policy for presentation to Governors;
  - taking due regard for government requirements and guidelines regarding the use of data;
  - policy implementation and monitoring including staff training;
  - ensuring that any Freedom of Information and subject access requests are responded to appropriately;
  - together with the Headteacher, responding appropriately to any data breaches in the school to ensure that the impact of such is minimised whilst maintaining an open and honest manner in informing the appropriate stakeholders of the breach.
- 2.2 Other staff have particular responsibilities for data handling and controls as specified in their job descriptions.
- 2.3 It must be emphasised however that all staff must have due regard to data policies in carrying out their day-to-day work.

**3. The General Data Protection Regulation (GDPR) – replacing the Data Protection Act (1998)**

- 3.1 The school complies with its duties under the GDPR (2018). The school is registered with the Information Commissioner's Office as a data controller.
- 3.2 Staff and governors should have due regard to the 6 principles of the Act. Data should be:
  - a) processed lawfully, fairly and in a transparent manner in relation to individuals;
  - b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
  - c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
  - e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;and

- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

#### **4. Data Processing Procedures**

- 4.1 The school only holds the data which it deems to be necessary to: facilitate and enhance teaching and learning and pastoral care; ensure the safety of students and staff; and carry out appropriate administration.
- 4.2 An information audit map will be carried out / updated once per year. This is known as the Information Asset Register (IAR)
- 4.3 A Data Protection Impact Assessment (DPIA) - sometimes referred to as a Privacy Impact Assessment (PIA) will be carried out as required but particularly when planning a new initiative that may involve ‘high risk’ data processing
- 4.4 Privacy notices, as show in the Staff and Student Privacy Notices (Appendix 2A and 2B), are issued annually to all staff and students (and a copy to parents of students in years 7 and 8), to inform them that the school holds data on them and who the school may share this information with.
- 4.5 All data that is gathered, whether relating to students, staff or other stakeholders, is kept as up-to-date and accurate as possible. Data collection sheets are issued to parents/carers for checking on a rolling program if required or the information is collected electronically were possible. When the school is informed of a change to personal data, computer and papers records are updated as soon as practical.
- 4.6 All staff and governors have a duty to ensure that data they hold is kept secure. Specific information regarding that can be found in the Acceptable Use Policy for Data (Appendix 1).
- 4.7 The school follows national guidelines regarding data retention. Paper copies of personal data will be shredded when no longer needed and electronic copies deleted. Hard drives are securely wiped when being disposed of. Educational records, including but not limited to SEN records, are stored until the student is 25, and then securely disposed of. Employee personnel records will be held for the length of employment plus 7 years, before being securely disposed of, with the exception of documents relating to child protection or accidents at work which may be held for longer periods.
- 4.8 With regards to subject access requests, whereby any student or member of staff may request access to his/her personal data, the school complies with the GDPR and follows guidance from the Information Commissioner’s Office. Access requests will be dealt with within one month of a written request being received. In the case of students making such a request, they will normally be given a copy of their data directly, unless the school feels that the student does not understand the nature of the request in which case this will be discussed with parents/carers, or the data is outside the provision of the GDPR.
- 4.9 Data may be shared with the Local Authority, DfE and other schools to allow the school to fulfil its statutory obligations, or to enable the transfer of information when a student leaves or joins the school. Details of who we share data and why are on the relevant Privacy Notice

#### **5. The Freedom of Information Act**

- 5.1 St Ivo School is committed to the Freedom of Information Act (2000) and to the principles of accountability and general right of access to information, subject to legal exemptions.
- 5.2 Under the Act, any person has a legal right to ask for access to information held by the school. They are entitled to be told whether the school holds the information, and to receive a copy, subject to certain exemptions. Requests under the Freedom of Information Act are different to subject access requests (see section 4.8 above).
- 5.3 The school routinely makes information available to the public as defined in the Information Commissioner’s Office model publication scheme. Much of this information can be found on the school website, or is otherwise available by contacting the school. Requests for other information will be dealt with in accordance with statutory guidance. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information.
- 5.4 Our process for responses to Freedom of Information requests is outlined in our Acceptable Use Policy for Data. We have a duty to respond to all requests within 20 working days (excluding school holidays).
- 5.5 Where information is subject to an absolute or qualified exemption under the Act, we will inform the person making the request of this, after invoking the public interest test procedures as appropriate. Any complaint made following this will be handled as per the school’s complaints procedure.
- 5.6 The Data Protection and Freedom of Information Officer must be made aware of all Freedom of Information requests. A register of these will be kept.

## 6. Use of CCTV

- 6.1 Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the GDPR and the Information Commissioner's Office (ICO) has issued a code of practice on compliance with legal obligations under that set of regulations.
- 6.2 The school uses CCTV equipment to provide a safer, more secure environment for pupils and staff and to prevent bullying, vandalism and theft. Essentially it is used for:
- The prevention, investigation and detection of crime.
  - The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
  - Safeguarding public, pupil and staff safety.
  - Monitoring the security of the site.
- The school does not use the CCTV system for covert monitoring.
- 6.3 Cameras are located in those areas where the school has identified a need and where other solutions are ineffective. The school's CCTV system is used solely for purposes(s) identified above and is not used to routinely monitor staff conduct. Cameras are only used in exceptional circumstances in areas where the subject has a heightened expectation of privacy e.g. changing rooms or toilets. In these areas, the school uses increased signage in order that those under surveillance are fully aware of its use.
- 6.4 The CCTV system is maintained by the school's premises and ICT teams, who periodically inspect the cameras to ensure that date and time references are accurate, clear images are recorded and that as far as possible equipment is protected from vandalism.
- 6.5 In areas where CCTV is used the school ensures that there are prominent signs in places which are clearly visible and readable, containing the school name, the purpose for using CCTV and a contact name.
- 6.6 The school's standard CCTV cameras record visual images only and do not record sound. Where two way audio feeds (eg call for help systems) are used, they will only be capable of activation by the person requiring help.
- 6.7 The school has notified the Information Commissioner's Office of the purpose for which the images are used. All operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the CCTV Code of Practice. Access to recorded images is restricted to staff that need to have access in order to achieve the purpose of using the equipment. All access to the medium on which the images are recorded is documented. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images. Under the Schools (Specification and Disposal of Articles) Regulations 2013, school staff can view CCTV footage in order to make a decision as to whether to search a student for an item. If the recorded footage reveals that theft has been committed by a member of staff, this evidence may be used in a disciplinary case.
- 6.8 Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified. Access to live images is restricted to reception staff, the ICT Technical Manager, Site Manager and members of the Senior Leadership Team unless the monitor displays a scene which is in plain sight from the monitoring location.
- 6.9 Recorded images can only be viewed by approved staff. The recorded images are viewed only when there is suspected criminal activity, or activity which could be harmful to students and staff, and not for routine monitoring of students, staff or visitors unless the camera(s) are installed to monitor the safe movement of persons through a designated area eg corridors (these areas will be identifiable by clear signs).
- 6.10 The school reserves the right to use images captured on CCTV where there is activity that the school cannot be expected to ignore such as criminal activity, potential gross misconduct, or behaviour which puts others at risk. The retention of recordings for evidential purposes will be authorised by the Headteacher or a member of staff to whom this authorisation has been delegated to by the Headteacher.
- 6.11 The school ensures that images are not retained for longer than is necessary. CCTV systems are designed to overwrite the oldest recordings after a set period.
- 6.12 Disclosure
- Disclosure of the recorded images to third parties can only be authorised the Headteacher or a member of staff to whom this authorisation has been delegated to by the Headteacher.
- Disclosure will only be granted:
- If its release is fair to the individuals concerned.
  - If there is an overriding legal obligation (eg information access rights).
  - If it is consistent with the purpose for which the system was established.
- All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented.

NB: Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

#### 6.13 Subject access requests

Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If the school receives a request, this will be handled as per section 4.8. As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and its disclosure is unlikely. Refusal to disclose images may also be appropriate where their release is likely to cause substantial and unwarranted damage to the individual, or to prevent automated decisions from being taken in relation to that individual.

## **APPENDIX 1 – ACCEPTABLE USE POLICY FOR DATA**

All staff and governors should be aware of this agreement, and agree to follow it as a condition of their employment or involvement with the school. Failure to do so may result in disciplinary action.

It is vital that the school fulfil its obligations under the General Data Protection Regulation (2018) and Freedom of Information Act (2000). All staff are given training on this, however this Acceptable Use Policy has been put together to ensure that all staff are aware of and follow specific rules.

### **Data to which this AUP applies**

1. Personal data is defined as data with two or more personal identifiers (e.g. name and address, name and date of birth).
2. Sensitive data is any data that could harm, discomfort or embarrass an individual if it were to become public or be made available to an unauthorised individual. For example SEN, racial or medical data, bank details, phone numbers.
3. This AUP also applies to other confidential data such as performance management documents.

### **Security of paper-based data**

1. Staff are responsible for ensuring that data issued to them remains secure. On site this means keeping data away from being easily accessible by unauthorised personnel e.g. students.
2. If taking data off site, paperwork should be stored securely at all times. You should remain with the data when in transit, and store it in a secure area e.g. a locked cupboard.
3. Data should never be taken outside of the EU.
4. Particularly sensitive data, e.g. SEN or medical records, payroll details etc, should never be removed from the school site and remain in a secure area e.g. locked cupboard, filing cabinet or office at all times.
5. All paper based records containing data should be securely shredded when no longer of use. You should not keep records beyond this time, unless advised otherwise (e.g. child protection records must be kept for longer).

### **Security of electronic data**

1. Ensure that your passwords for access to the network, email, SIMS and Go4Schools are strong passwords. You should change these on a regular basis, and not tell other members of staff or students your passwords.
2. Ensure that you lock or log out your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes places using your credentials, which can be monitored.
3. When storing data in Projects (the network shared area) ensure that this cannot be accessed by students. Name files appropriately.
4. Ensure that data is not visible to students or other unauthorised personnel. This includes any data in SIMS.net and Go4Schools.
5. Data must not be stored on staff laptops or any electronic device outside of school without being encrypted and must comply with the GDPR. In general there should be no need to store data outside school.
6. If storing/transferring data using a removable device, this device must be an encrypted USB drive which will be supplied to you by the school on request. This USB drive should remain physically secure both in transit and when stored, in the same way as paper based records. It must not be taken out of the EU. Should this USB drive go missing, you must inform a Senior Leader immediately. When your employment with the school terminates, you should return the USB drive to the ICT Technical Manager for secure disposal. Data must not be copied from the encrypted USB drive onto any computer equipment used off school site (this includes home computers).
7. Photos and videos of students must only be taken using school owned devices. Any exception to this can only be authorised by the Headteacher or the Director of School Strategic Operations (DSSO). The placing of photos on websites and social media must be approved by the Headteacher or a member of staff to whom this approval has been delegated to by the Headteacher.
8. Files should be deleted from the network and encrypted USB drives when no longer needed, in line with the school's data retention policy. When deleting a file from a USB drive outside of school you should use shift and delete to avoid the risk of a copy of the file being stored in the recycle bin.

9. If you use your mobile device(s) to access school email you must make sure that they are protected with a password or pass-code logon. If your device is lost or stolen you must inform the Data Protection Officer or the Director of School Strategic Operations as soon as possible.
10. When you leave the school, be aware that your accounts for the network, email and other systems will be disabled when your contract ends.

### **Release of data to others**

1. Staff may share information with each other regarding students as necessary in the performance of their duties, as long as this sharing of information is in the best interests of the students. The only exception to this is where a manager has explicitly stated that information is not to be shared.
2. When sharing data with another organisation e.g. another school, you should check the legitimacy of the potential recipient. Wherever possible, school-to-school student data transfers will be made by the data admin staff using the secure B2B and S2S systems. If you are unsure you should consult a Senior Leader, and always check before sending data out of the country.
3. Staff with access to data regarding other staff, such as contracts and pay scales, should ensure they have been granted permission to access this data by the Head or Deputy Head.
4. You should use your school provided email account for all email related to your work for the school. This system is managed by the County Council. When emailing a non stivoshool.org address, emails will pass outside of the County security systems and therefore you should not send data to such an address without prior approval from a member of Senior Leadership.
5. The school takes any data breach very seriously. Should you become aware of any such breach, or the potential for one, you should inform a Senior Leader immediately.

### **Freedom of Information and Subject Access Requests**

1. Any member of staff or the Governing Body may receive a subject access request for personal data, or a request for information under the Freedom of Information Act. Such requests will be made in writing or by email.
2. If you receive such a request, you should inform the Data Protection and Freedom of Information Officer immediately, or in his/her absence the Headteacher. The school has a legal duty to respond to requests within a time limit, so it is important that you pass on the request in a timely manner.
3. You should then await a response for the Data Protection and Freedom of Information Officer or Headteacher before sending a response to the request.
4. Staff should be aware that, in fulfilling requests, the school may be required to disclose the contents of emails. It is therefore vital that staff remain professional in all correspondence.
5. It is an offence to wilfully conceal, damage or destroy information in order to avoid responding to an enquiry, so it is important that no records that are the subject of an enquiry are amended or destroyed.

## **Privacy Notice – General Data Protection Regulation (2018) – For the school workforce (those employed or otherwise engaged to work at a school)**

We, St Ivo School, are the Data Controller for the purposes of the GDPR.

Personal data is held by the school about those employed or otherwise engaged to work at the school or Local Authority. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modeling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teachers' Review Body.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

The school uses CCTV systems for the prevention, investigation and detection of crime, the apprehension and prosecution of offenders, safeguarding public, pupil and staff safety and monitoring the security of the site.

### **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. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

### **Storing this information**

We hold school workforce data for 7 years.

### **Who we share this information with**

We routinely share this information with:

- **The Local authority**

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

- **Department for Education (DfE)**

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

- **Education Personnel Management (EPM)**

We share personal data with EPM for Human Resource and Payroll purposes.

***We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.***

## Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

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

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

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

## Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the school office.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the data protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

**I have read and understood the regulations regarding the use of my personal data.**

Signed: \_\_\_\_\_

Date: \_\_\_\_\_



## Privacy Notice – General Data Protection Regulation (2018) – For all students at St Ivo School

St Ivo School is the data controller for the purposes of the General Data Protection Regulation Act. We collect personal information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data to:

- Support your learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well we are doing.

### Information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- Special Educational Needs information
- Behavioural information including exclusions
- Post 16 Learning information and destinations

We store this data securely during your time at school and beyond for purposes of references, results checking etc.

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide the names and addresses of you and your parent(s), and any further information relevant to the support services' role. We may also share data with post 16 providers to secure appropriate support on entry to post 16 provision.

However, parent(s) can ask that no information beyond names, addresses and your date of birth be passed to the support service. This right transfers to you on your 13th birthday. Please tell the School Secretary if you wish to opt out of this arrangement. For more information about young people's services, please go to the National Careers Service page at <https://nationalcareersservice.direct.gov.uk/aboutus/Pages/default.aspx>

***We will not give information about you to anyone without your consent unless the law and our policies allow us to.***

The school uses CCTV systems for the prevention, investigation and detection of crime, the apprehension and prosecution of offenders, safeguarding public, pupil and staff safety and monitoring the security of the site.

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use of the Local Authority. This is a statutory requirement and underpins school funding and monitoring (regulation 4 of The Education (Information About Individual Pupils) (England) Regulations 2013). To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

### **The National Pupil Database (NPD)**

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

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

### **Requesting access to your personal data**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, please contact the school secretary.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

### **Contact**

If you would like to discuss anything in this privacy notice, please contact the School Secretary

**I have read and understood the regulations regarding the use of my personal data.**

Signed: \_\_\_\_\_

Date: \_\_\_\_\_