



DIOCESE OF CHICHESTER  
ACADEMY TRUST

# DATA PROTECTION POLICY

<b>Date Agreed:</b>	<b>September 2022</b>
<b>Review Date:</b>	<b>September 2024</b>
<b>Type of Policy:</b>	<b>DCAT Statutory Policy</b>

Revision Number	Date Issued	Prepared by	Approved	Personalised by school	Comments
5	Sept 2022	Handsam / JS	Trust Board		Handsam (DPO) model policy adapted for Trust
4	June 2021	DCAT	Trust Board		DPO
3	June 2020	CF			DPO
2	May 2018	SJP/DC			JUDICIUM
1	May 2017	SJP	DCAT Directors		

<i>Type of Policy</i>	<i>Tick ✓</i>
DCAT Statutory Policy	✓
DCAT Non-statutory Policy	
DCAT Model Optional Policy	
School Policy	
Local Authority Policy	

## Contents

Introduction .....	1
UK GDPR Adequacy Decision .....	2
1. Policy Aims .....	3
2. What is Personal Data and Sensitive Personal Data .....	3
3. Lawful Processing .....	3
4. Data Subjects .....	4
5. Data Held .....	4
6. Responsible Persons .....	4
Data Controller .....	4
(Data Protection Manager) or appropriate title – e.g. Office Manager .....	5
7. ICO Registration .....	5
8. Access to Information .....	5
9. Safe and Secure Storage of Files and Data .....	6
10. Documentation and Record Keeping .....	6
11. Right to Rectification .....	6
12. Right to Portability .....	7
13. Data Protection on the Move .....	7
14. Data Retention .....	7
15. Privacy Notices .....	7
16. Data Destruction .....	7
17. Data Protection Impact Assessment (DPIA) .....	8
18. Breaches .....	8
Internal Breach Register .....	8
Notification of Breaches to the ICO .....	8
19. Staff Recruitment .....	9
Checks .....	9
Shortlisting .....	9
Interviews .....	9
Retention of Information .....	9
20. Successful Candidates .....	10
References .....	10
Gaining Consent .....	10
21. Employment Records .....	10
22. Pension and Insurance Schemes .....	10
23. Equal Opportunities Monitoring .....	10

24.	Marketing Material .....	11
25.	Fraud Detection .....	11
26.	Disclosure Requests .....	11
27.	Performance Management Records.....	11
28.	Monitoring the Use of Electronic Communications .....	11
29.	Information about Employees' Health .....	12
30.	Sickness and Ill-health Records.....	12
31.	Occupational Health Schemes .....	13
32.	Medical Examinations .....	13
	Recruitment.....	13
	Current Employees.....	13
33.	Monitoring and Review .....	13
	Appendix 1: Roles.....	14
	Appendix 2: Privacy Notice Template.....	15
	Appendix 3: Data Protection Impact Assessment Template.....	16
	Appendix 4: Internal Breach Register Template.....	17
	Appendix 5: Breach Notification Supervisory Authority .....	18
	Appendix 6: Legitimate Interest Assessment Template .....	20

## Introduction

Our **vision** for our Trust is we exist to:

***Help every child achieve their God-given potential***

Our **aims** are clear. We aim to be a Trust in which:

**D**eveloping the whole child means pupils achieve and maximise their potential

**C**ontinued development of staff is valued and improves education for young people

**A**ll schools are improving and perform above national expectations

**T**he distinct Christian identity of each academy develops and is celebrated

Our work as a Trust is underpinned by shared **values**. They are taken from the Church of England's vision for Education and guide the work of Trust Centre team. They are:

### **Aspiration**

I can do all things through Christ who strengthens me  
(Philippians 4 vs 13).

### **Wisdom**

Listen to advice and accept discipline, and at the end you will be counted among the wise  
(Proverbs 19 vs 20)

### **Respect**

So in everything do to others what you would have them do to you  
(Matthew 7 vs 12)

Our vision of helping every child achieve their God-given potential is aligned with the Church of England's vision for education and is underpinned by the Bible verse from John: *I have come that they may have life, and have it to the full.*

## UK GDPR Adequacy Decision

On 28th June 2021, the European Union (EU) formally recognised the UK's high data protection standards after more than a year of talks. This will allow the continued seamless flow of personal data from the EU to the UK. This means that if your educational facility receives personal data from the EU or EEA it can continue to flow as before and you do not need to take further action, unless the data falls within the scope of the DPA 2018 immigration exemption.

The EU GDPR is an EU Regulation and it no longer applies to the UK. If you operate inside the UK, you need to comply with the Data Protection Act 2018 (DPA 2018).

In practice, there will be very little change to the core data protection principles, rights, and obligations. Schools will not need to make any new arrangements if they currently transfer data from the UK to the EEA. Unless your facility holds or processes data transferred for the purposes of immigration control (or data that otherwise falls within the UK immigration exemption), data can still flow freely from the EEA.

The UK will retain this status for four years, but the European commission warned that it could be withdrawn at any time if UK law was no longer deemed to offer EU citizens protection over how their data was used.

Only 12 countries, including Canada, Switzerland and New Zealand, have received positive adequacy decisions from the EU. The US was judged "partially adequate", but this decision was overturned twice by the European court of justice.

## 1. Policy Aims

Personal data of employees and candidates will be processed lawfully, fairly and in a transparent manner, collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The data retained will be accurate and, where necessary, kept up to date, in a form which permits identification of data subjects for no longer than is necessary and 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.

## 2. What is Personal Data and Sensitive Personal Data

The ICO defines Personal Data as:

- Personal data is information that relates to an identified or identifiable individual.
- What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.
- If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
- If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

The ICO defines Sensitive Personal Data (also known as 'Special Category Data') as:

- Special category data is personal data that needs more protection because it is sensitive;
- In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked;
- There are 10 conditions for processing special category data in Article 9 of the UK GDPR (see 'Lawful Processing' below);
- You must determine your condition for processing special category data before you begin this processing under the UK GDPR, and you should document it.

## 3. Lawful Processing

Article 9 of the Data Protection Act 2018 prohibits the processing of Sensitive Personal Data (also known as 'Special Category Data'). There are 10 exceptions to this general prohibition, usually referred to as 'conditions for processing special category data':

- (a) Explicit consent
- (b) Employment, social security and social protection (if authorised by law)
- (c) Vital interests
- (d) Not-for-profit bodies
- (e) Made public by the data subject
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)
- (h) Health or social care (with a basis in law)
- (i) Public health (with a basis in law)
- (j) Archiving, research and statistics (with a basis in law)

Five of the conditions only apply if processing has an authorisation or basis in UK law as set out in the Data Protection Act 2018.

In order to meet its obligations The Diocese of Chichester Academy Trust (DCAT) will keep a record of all types of data, the purposes for which it is kept and the conditions under which it is being lawfully processed. This will be done using the template in Appendix 6: Legitimate Interest Template, which must be reviewed three times per year for veracity and any necessary changes made by the **(DATA PROTECTION MANAGER)**.

## 4. Data Subjects

DCAT is responsible for any and all data held within its remit for any Data Subject, which may include, but not be limited to, those natural persons, such as:

- Staff
- Members, Trustees and Governors
- Trust Employees
- Pupils
- Parents
- Carers
- Emergency Contacts
- Contractors

## 5. Data Held

DCAT holds data in a wide range of forms and formats, which may include, but not be limited to:

- Hard copy
- Electronically in Trust and ST Blasius systems
- Electronically in third party systems

## 6. Responsible Persons

### Data Controller

The Data Controller of DCAT and ST Blasius is responsible for:

- The adherence to data protection law and the safety of processing activities on site;
- Ensuring safe and confidential systems are in place in ST Blasius and consulting the Data Protection Officer, Handsam Ltd, in the implementation, development and monitoring of data processing activities;
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented to the personal data processed; and
- Providing information to bodies entitled to receive information under data protection law.

### **(Data Protection Manager)**

**Will ensure that high standards of data security and confidentiality are maintained at all times on site;**

- Will coordinate, monitor and oversee appropriate training in data management and encourage a positive data culture;
- Will consult with employees and their representatives with regard to putting data protection procedures in place and monitoring them;
- Will ensure all staff are aware of St Francis's data on the move procedures; and
- Will advise on data issues and will assess the severity of data breaches and respond accordingly.

## **7. ICO Registration**

DCAT as a Data Controller will register with the ICO and pay the relevant fee. The ICO certificate shall be shared with all schools to be displayed at reception. The ICO's processes for renewal shall be followed each year. See: <https://ico.org.uk/for-organisations/data-protection-fee/> and shall not be allowed to lapse.

## **8. Access to Information**

All employees have a right to know the nature and source of information kept about them. Each member of staff at ST Blasius will be provided with personal details to check regularly, at times determined by the **DATA PROTECTION MANAGER**. The contract based Privacy Notice will also serve as a referenceable document for this information.

Any person who is a Data Subject may make a Subject Access Request at any other time to see the information kept about them and in order to verify accuracy. Data Subjects can make representations to the **DATA PROTECTION MANAGER** about information being retained that is inaccurate or is of a sensitive personal nature.

Employees have the right to apply for access to information required for a discipline, capability or grievance hearing (unless the provision of such information might prejudice criminal investigation). The records kept should only be sufficient to support conclusions drawn. Unsubstantiated allegations should be removed.

Spent discipline warnings will be retained on the member of staff's personnel file.

ST Blasius will respond to any Subject Access Request without undue delay and provide information within one month free of charge. Requests must be made in writing.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, ST Blasius reserves the right to either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

ST Blasius shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. Additional terms for [exemptions](#) of requests have been added by the *Data Protection Act 2018*, including child protection data, data which can cause serious harm to a subject or data active in



court proceedings. A decision to deny a request or impose a fee will be reasoned and the subject notified within one month of receipt.

Where ST Blasius has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

## 9. Safe and Secure Storage of Files and Data

The **DATA PROTECTION MANAGER** will take necessary precautions to ensure that both electronic and manual files are secure. This shall include password protection and encryption as standard on all devices which hold or have access to personal or sensitive personal data as defined under the Data protection Act 2018.

No manual or electronic files will be taken off the premises except in an emergency, or when expressly authorised by the **DATA PROTECTION MANAGER** who will ensure that employees who are affected are notified and given an opportunity to make representations to him/her. This includes information held on personal computers and portable computing devices, including mobile phones and memory sticks. This list is not exclusive.

Manual files will be stored in a safe and secure lockable cabinet at all times. ST Blasius will adopt the National Cyber Security Centre's guidance [10 Steps to Cyber Security](#) in the safe and secure storage of electronic files and data. ST Blasius will therefore:

- Protect networks from attack and monitor and test security controls in place to achieve this;
- Ensure users are educated, trained and aware;
- Produce and establish anti-malware defences across the school;
- Produce a policy to control all access to removable media;
- Apply security patches and ensure secure configuration of all systems is maintained;
- Establish effective management processes, limit user privileges and monitor user activity appropriately;
- Establish an incident response and disaster recovery capability;
- Establish an effective monitoring strategy of all systems and networks; and
- Develop and implement a policy on the use of mobile phones and train staff to adhere to it.

## 10. Documentation and Record Keeping

Under the *General Data Protection Regulation* and the *Data Protection Act 2018*, records of processing must be retained. ST Blasius will hold compliant and comprehensive processing records in relevant fields, covering the nature of the data, the purposes of processing, any recipients, security measures, retention times and controller information.

## 11. Right to Rectification

ST Blasius shall ensure that any request by a Data Subject to have incorrect data held rectified shall be delivered in a timely manner, in a period not longer than 28 days. This process shall be managed by the **DATA PROTECTION MANAGER**

## 12. Right to Portability

ST Blasius shall ensure that any request by a Data Subject to have data held about them moved to a third party takes place in a timely manner between the parties involved and by a safe and secure transfer method, to be agreed between the parties involved.

## 13. Data Protection on the Move

The loss of data outside the immediate school environment can be the most serious and costly.

The **DATA PROTECTION MANAGER** of ST Blasius will ensure that all staff are aware of the dangers of taking data off the school's immediate environment and are aware of the procedures in place to minimise the risk.

All devices storing data such as laptops and any work phones must be password protected and data encrypted. Staff will not remove any more data than is necessary from the ST Blasius premises and will consult the **DATA PROTECTION MANAGER** regarding the specific data movement requirements of their role.

## 14. Data Retention

The Trust and its schools will adhere to all specified data retention periods. To achieve this the Trust will follow the timeframes specified in the document 'IRMS Retention Policy', the most recent version of which is to be found:

<https://irms.org.uk/page/SchoolsToolkit>

This process will also serve to cause the Data Minimisation required by the Data protection Act 2018 to take place.

## 15. Privacy Notices

As required by the Data Protection Act 2018, ST Blasius will display a Privacy Notice, or reference to where it can be read, at all points that data can be collected or displayed, including, but restricted to:

- Website
- Online systems
- Staff contracts
- Student/Parents forms
- Recruitment forms

## 16. Data Destruction

ST Blasius will ensure that once a specified data retention period has passed that all such data is safely destroyed. Processes shall include:

- For physical documents: Shredding
- For digital data: Wiping with confirmation statement/certificate to be held in perpetuity
- For disposal of IT equipment of any kind: Use of an accredited specialist provider with confirmation statement/certificate to be held in perpetuity

The Data Protection Manager shall take charge of ensuring that all aspects of data across all areas of the organisation are considered for this process once per term (i.e. three times per year).

## 17. Data Protection Impact Assessment (DPIA)

Each time the Trust or ST Blasius or any of its staff consider changing or introducing a practice for managing data in any form, a Data Protection Impact Assessment (DPIA) shall be conducted using the form at Appendix 2. Such assessment will also include an Equality assessment in line with the Trust and ST Blasius Equality Policy.

## 18. Breaches

All staff and other covered by this policy must report data breaches of any kind, no matter how small or unsubstantial they appear, to the **DATA PROTECTION MANAGER** of ST Blasius Advice, if required, will be sought from the Trust DPO, Handsam Ltd. This shall be done in writing via email to: [info@handsam.co.uk](mailto:info@handsam.co.uk).

Data breaches which pose a risk to individuals must be notified to the supervisory authority within 72 hours and the affected individuals without undue delay. If there is a delay this must be justified.

The **DATA PROTECTION MANAGER** of ST Blasius shall ensure that all the affected individuals are informed in writing or by telephone and then in writing, if that is deemed to be the best way of getting the information to them quickly.

### Internal Breach Register

The **DATA PROTECTION MANAGER** of ST Blasius shall be responsible for the maintenance of an internal Breach Register.

### See Appendix 4 for a Breach Register Template

This register shall be reviewed three times per year to aid the improvement of data processing and practice.

### Notification of Breaches to the ICO

Data breaches which pose a risk to individuals must be notified to the supervisory authority within 72 hours and the affected individuals without undue delay. If there is a delay this must be justified.

An assessment tool of what should be reported to the ICO can be found on their website: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

The **DATA PROTECTION MANAGER** of ST Blasius shall ensure that the ICO are formally informed of any substantial breach by calling the ICO helpline – **0303 123 1113**.

The information which will need to be provided includes:

- What has happened;
- When and how you found out about the breach;
- The people that have been or may be affected by the breach;

- What you are doing as a result of the breach; and
- Who we should contact if we need more information and who else you have told.

The information provided shall be both accurate and fulsome.

The ICO will send a copy of the information submitted in writing, which should be filed alongside the Internal Breach Register to form a Substantive Breach Register.

## 19. Staff Recruitment

In advertising for posts, ST Blasius will include a Privacy Notice detailing what personal data or sensitive personal data will be gathered, how it will be held, processed and disposed of. The notice will also inform individuals of their data rights.

Within St Francis, the **DATA PROTECTION MANAGER** will determine who may have limited access to this information and will inform the person(s) concerned that this is being done.

ST Blasius will not collect more personal information than is necessary for the recruitment process. Information collected will not be irrelevant or excessive.

### Checks

Disclosure and Barring Service (DBS) checks will be carried out in line with statutory responsibilities under the *Safeguarding Vulnerable Groups Act 2006*, as amended by the *Protection of Freedoms Act 2012* and statutory guidance in [Keeping Children Safe in Education](#).

Any other vetting which is required by law will be carried out as necessary and in line with current legislation and policy.

Checks to verify the qualifications and fitness to teach (or to support teaching) will also be carried out. Other checks may be carried out to verify information provided by candidates for posts.

### Shortlisting

Candidates will be informed that the selection panel will have access to the information provided in the application and any references/testimonials received.

### Interviews

Only the information relevant to the recruitment process (and information that may be required in defence against any discrimination claims) will be retained confidentially on the individuals personnel file. They will also be told that they can obtain (from the **DATA PROTECTION MANAGER**) copies of any panel interview notes concerning them personally that are retained by the school.

All other interview material will be destroyed immediately after the interview.

### Retention of Information

The information of unsuccessful candidates obtained for recruitment purposes at ST Blasius will be retained for 6 months before secure disposal.

A secure central record that will list all checks carried out will be kept for the purposes of inspection and to assure governors that records have been checked.

All candidates will be asked whether they want their information kept on file for possible future vacancies. Consent to this will be in an auditable form.

## 20. Successful Candidates

On assumption of a role at ST Blasius the forms of personal data which will need to be processed and gathered for the performance of the role will be outlined to the individual in a Privacy Notice within their contract. This data will include verified references and an up to date DBS check. This data will be securely held and subject to the following employee data retention periods – personnel files will be retained for 6 years from the date of resignation.

### References

Candidates do not have the right to obtain access to a confidential reference from the school/organisation giving it, but no such exemption exists for the prospective employer.

ST Blasius will not provide confidential references to other institutions/organisations about an employee at St Francis, unless the employee requests one in writing for good reason.

### Gaining Consent

Where required, requests for consent to personal data processing will be intelligible, easily accessible, in plain language and with the purpose for the data processing stated and evident. Consent will cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent will be gathered for all of them.

Consent gathered will be held securely in a clear and auditable form. Subjects will be able to be withdraw consent through the same medium it was given. If consent is withdrawn, this does not necessarily make the processing unlawful, this must be noted if applicable in the consent request.

## 21. Employment Records

ST Blasius aims to balance its need to keep records and the employee's right to a private life.

## 22. Pension and Insurance Schemes

Information may be supplied to a third party for pensions and insurance schemes, where such information is necessary. Consent will be secured from employees concerned and processing agreements established with third parties detailing how data will be secured and processed.

## 23. Equal Opportunities Monitoring

Information on staff is periodically required by the government This is sensitive personal data, and the information will be kept to a minimum, and as far as possible, in an anonymous form. [DATA PROTECTION MANAGER](#) will ensure that high standards of data security and confidentiality are maintained at all times. Staff will have a full awareness of this form of personal data processing on assumption of job role through contract and Privacy Notice.

## 24. Marketing Material

No information about employees ST Blasius will be provided to marketing companies, unless the person(s) concerned have given explicit and auditable consent.

## 25. Fraud Detection

Data matching for fraud detection (e.g. to detect whether the employee is receiving state benefits or not) are possible. Before the employer consents to the school participating in such a scheme, the staff will be consulted. New employees must then be told of this scheme, and all employees should be reminded of it periodically under arrangements made by the [DATA PROTECTION MANAGER](#) and approved by the employer.

## 26. Disclosure Requests

Members of staff who receive requests for references or other information about members of the current or previous employees at ST Blasius should inform the [DATA PROTECTION MANAGER](#) before providing the information to ensure that they are acting within the law and official guidance.

## 27. Performance Management Records

Performance reviews will be carried out on all staff in accordance with the DCAT Performance Management Review (Appraisal) Policy.

The reports on teaching staff performance obtained through the annual formal performance management system will be retained by the Headteacher (with a copy to the member of staff concerned). Only details about professional development needs/requests may be shared with other staff.

ST Blasius has the same arrangements in place for performance records of all staff.

## 28. Monitoring the Use of Electronic Communications

The Trust will keep all monitoring at work within the provisions of the *General Data Protection Regulation 2016* and the *Data Protection Act 2018*.

ST Blasius will not intrude into the private lives of staff, but reserves the right to monitor the use of all electronic devices issued or made available by the ST Blasius such as school computers, laptops, video and audio machines, phones and fax machines. This will only be done where there is a good reason to do so and appropriate records will be kept, which can be accessed by staff (and pupils) on request to the [DATA PROTECTION MANAGER](#)

All monitoring will be conducted in accordance with the powers of an employer under the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, which permits an employer to vet communications without the consent of the caller, writer or recipient where the intention is:

- To establish the existence of facts applicable to the business;
- To ascertain compliance with regulatory or self-regulatory practices or procedures which are applicable to the system controller in the carrying on of his business, or applicable to

another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures;

- To ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties;
- In the interest of national security;
- For the purpose of preventing or detecting crime;
- For the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system;
- In order to secure or as an inherent part of the effective operation of the system;
- Monitoring communications for the purpose of determining whether they are communications relevant to the system controller's business; and
- Monitoring communications made to a confidential voice-telephony counselling or support service which is free of charge (other than the cost, if any, of making a telephone call) and operated in such a way that users may remain anonymous if they so choose.

All staff are advised that such monitoring might take place at ST Blasius for these purposes including for the misuse ST Blasius equipment or its use for inappropriate purposes.

The employer will establish with the [DATA PROTECTION MANAGER](#) after consultation with the staff, a policy on how telephones/fax and computers may be used for any private communications. Breach of this code once established will be a discipline offence.

## 29. Information about Employees' Health

ST Blasius that data relating to an individual's health is classified as sensitive. Data of this nature will be managed with a constant awareness of data protection in a confidential and secure manner. Concerns regarding how data is managed should be reported to the [DATA PROTECTION MANAGER](#)

Any data on an employee's state of physical or mental health is sensitive personal data and will only be kept when the employee has been told what information is involved and the use that will be made of it, in addition to security arrangements. The information will only be retained for a set period and in accordance with employee consent and data rights. Only necessary and limited individuals at ST Blasius will be able to access this information where they genuinely need it to carry out their job.

## 30. Sickness and Ill-health Records

As far as possible, ST Blasius will only retain information that is necessary to establish an employee's fitness for work, securely and for a set period. The employer has delegated to the [DATA PROTECTION MANAGER](#) the responsibility for determining what is necessary.

ST Blasius recognises the difference between a 'sickness or injury record' and an 'absence record'.

Sickness or injury records contain sensitive personal information. They will only be kept for specific purposes with the written auditable consent of the employee, e.g. in the case of capability or absence through ill-health proceedings. However, this does not prevent ST Blasius from recording that sickness notes have been received and the dates of the absence.

Absence records may only give the reason for ill-health absence as 'sick' or 'accident' or 'injury', without referring to the specific condition. No information about any of the above records will be

made available to other employees unless cleared by the **DATA PROTECTION MANAGER** as necessary.

### 31. Occupational Health Schemes

ST Blasius will operate within the rules of any scheme to which it belongs. All staff will be informed about how health information will be used under the scheme and who will have access to it. A processing agreement with the scheme will be secured to this end.

Details are contained in the Employee Handbook.

### 32. Medical Examinations

#### Recruitment

Job applicants must only be medically examined to:

- Ensure they are medically fit for the specific role;
- Meet legal requirements; and
- Determine the terms on which they are eligible to join a pension or insurance scheme.

**St Francis** will make it clear during the recruitment process if tests are required for the role.

#### Current Employees

Medical information will only be obtained through examination or testing if:

- The tests are part of a voluntary occupational health and safety programme;
- Necessary to prevent a significant health risk;
- Needed to determine an employee's continuing fitness for the role;
- Needed to determine whether an employee is fit to return to work after a period of absence;
- Needed to determine an employee's entitlement to health-related benefits; or
- Needed to prevent discrimination on the grounds of disability, or to assess the need to make reasonable adjustments, or to comply with other legal obligations.

### 33. Monitoring and Review

The Trust will monitor the implementation of the policy and register annually with the Information Commissioner's Office.

The Headteacher and **DATA PROTECTION MANAGER** will monitor the effectiveness of the policy and will report to the Local Governing Body and Trust at least annually.

The Trust will review this policy at least every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the Trust schools.



## Appendix I: Roles

Role	Person	Email	Telephone
<b>Data Protection Officer (DPO)</b>	<b>Handsam Ltd</b> Office 27 East Moons Moat Business Centre. Oxleaslow Road, Redditch, Worcestershire, B98 0RE	<a href="mailto:info@handsam.co.uk">info@handsam.co.uk</a>	03332 070737
<b>Data Manager(s)</b>	<b>Jo Rooney</b>	<b>Office@stfrancisventnor.org</b>	<b>01983844379</b>

## Appendix 2: Privacy Notices

- [Staff, Governors & Volunteers – October 2022](#)
- [Pupils, Parents and Carers – August 2022](#)

## Appendix 3: Data Protection Impact Assessment Template

DATA PROTECTION IMPACT ASSESSMENT					
PROCESSING DETAILS					
SCALE, SCOPE AND CONTEXT	PURPOSE AND PROCESSING OPERATION	NATURE OF PERSONAL DATA	PERIOD OF RETENTION	DATA ASSETS e.g. networks or hardware	COMPLIANCE WITH APPROVED CODES OF PRACTICE
NECESSITY AND PROPORTIONALITY					
LAWFULNESS OF PROCESSING	PRIOR CONSULTATION	DPO ADVICE	RISK TO RIGHTS AND FREEDOMS OF DATA SUBJECTS	LIKELIHOOD OF BREACH AND IMPACT (1-5)	
MANAGEMENT OF RISK					
MEASURES TAKEN TO REDUCE RISK	COMPLIANCE DEMONSTRATION	DOCUMENTATION	MONITORING AND REVIEW		

## Appendix 4: Internal Breach Register Template

INTERNAL BREACH REGISTER					
Date	Details of breach	Consequences (Subject and controller impact)	Action taken	Timescale	Notification to authority and/or subject

## Appendix 5: Breach Notification Supervisory Authority

BREACH NOTIFICATION SUPERVISORY AUTHORITY			
<b>Controller name:</b>			
<b>DPO name and contact:</b>			
<b>Date and time of breach:</b>			
<b>Date and time of notification:</b>			
<b>Nature of breach:</b>			
<b>Categories of personal data affected:</b>			
<b>No. of subjects affected:</b>			
<b>No. of records affected:</b>			
<b>Subjects notified:</b> (Communication affixed)	YES		NO
	Reasons for non-notification:		
<b>Potential and realised consequences:</b>	(Cover subjects and controller)		
<b>Security measures in place:</b>			

<b>Security measures to be implemented in response:</b>	
---	--

## Appendix 6: Legitimate Interest Assessment Template

LEGIMATE INTEREST ASSESSMENT				
Nature of processing	Controller interests	Impact on the rights and freedoms of subjects	'Reasonably' expect data to be processed on this basis?	Implications for child data (If applicable)