St Francis Church of England Voluntary Aided Primary School

Data Protection Policy

(with regard to The General Data Protection Regulations 2018)

Policy drawn up by Administrator
ratified by Governors

Date 5/1/2016

Version No	Date	Change/Review
V1.0	January 5th 2016	Policy Adopted
V1.1	February 2018	Amended ref GDPR
V1.2	May 15th 2018	Ratified
V1.3	November 2018	Review due

Data Protection

This document is a statement of the aims and principles of St Francis School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

This policy should be read in conjunction with the following:

- St Francis Personal Data Management and Security Policy
- E-Safety Policy
- Business Continuity Plan
- ICT Disposal Policy
- St Francis Risk Assessment Register
- Freedom of Information Policy

All of these facilitate the incorporation of the GDPR's Privacy by Design principle into the everyday running of St Francis Nursery and School.

Introduction

St Francis Primary School needs to keep certain information about its employees, pupils and other adults working or volunteering in the school, in order to monitor performance, achievements, and health & safety.

It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. In order to do this, St Francis Primary School, so far as is reasonably practicable, complies with the data protection principles, as contained in the Data Protection Act and the 2018 GDPR.

In summary these principles state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner not in line with that purpose with consent for that processing from the individual or their representative
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be securely protected from unauthorised access, accidental loss or destruction.
- Be stored only in countries within the EU, EEA (European Economic Area) or with companies that comply with the EU's Data Protection Directive.

St Francis Primary School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens the School has developed this Data Protection Policy.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers
The school as a corporate body is the Data Controller, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters. The school has Designated Data Controllers:
the Headteacher, Office Manager, the administrative assistants and the ICT Associate.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal or sensitive data about himself or herself or their child should raise the
matter with the Office Manager.

Responsibilities of Staff
All staff are responsible for:

- Ensuring that any information that they provide to the school in connection with their employment is accurate and up to date.
- Informing the school of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a pupil's assessment data, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the GDPR.

Data Security
(see also Personal Data Management and Security Policy)

All staff are responsible for ensuring that:

- Any personal and sensitive data that they hold is kept securely.
- Personal and sensitive information is not disclosed either orally, in writing, via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal and sensitive information should:
- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe and password protected.

Rights to Access Information
Under the GDPR all staff, parents and other users are entitled to:

- Know what information the school holds and processes about them or their child and why
- upon request, see what data is processed

- Know how to keep their data up to date
- ask for their data to be erased
- decide to move their data to another processor to whom St Francis must then supply the data (the right to *portability)
- object to St Francis' use of their data. Immediately that an objection is raised in writing, St Francis must stop the processing of the stated data unless there is an overriding legitimate reason to continue
- demand that any automated decision about the individual be reviewed by a human. At St Francis, however, no automatic decisions are made in this way
- Know what the school is doing to comply with its obligations

(*portability means that the school will have to provide requested information electronically and in a commonly used machine readable format)

Subject Access Requests (SAR)

All staff, parents and other adults have a right under the 1998 Act and the 2018 GDPR to access personal data being kept about them or their child either electronically or in paper files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to School Office.

(Please refer to the Freedom of Information Policy for further information).

The school will, upon this written request, first check the identity of the requester. Should identity be verified, it will provide staff, parents or other relevant adults with the personal data held about them or their child/ren. This will state all the types of data the school holds and processes about them, and the reasons for which they are processed as well as the retention period for that data and ways in which it could be corrected by the subject, and where this data may be shared by St Francis School.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the mandatory 30 school days, as required by the GDPR. Should the request be made prior to a school holiday, the thirty days will continue after the return to school.

Should another individual's details be contained within documentation necessary for a SAR, redaction will be used to blank out these details and a copy of the redactions held by school.

Manifestly unfounded or excessive requests can be refused, and St Francis will outline the basis for the refusal in writing to the requester. The requester will then have the right to complain directly to the ICO.

A subject access request is processed free of charge by St Francis School.

St Francis Subject Access Request Form

Name …….. Date ……

Address ……..

……..

Contact tel ……..

Email ……..

Please tick how you would like the response to this request communicated to you:

- ☐ Post
- ☐ Email
- ☐ Via your child's bookbag

Whose personal data are you requesting?

- ☐ yourself
- ☐ your child Name …….
- ☐ your child Name ……..
- ☐ your child Name ……..

NB.
St Francis School must respond with the following information: what personal data is held and why, how it is being processed, the retention period and how an individual can correct inaccurate data.

SAR REGISTER

Date	Request made by	Info provided by	Information provided/in what format	Date sent to subject	Initials

Subject Consent

In many cases, the school can only process personal data with the consent of the individual.

Where there is personal data that does not fall into the category of having a legal basis, schools must seek the consent of the individual to process it, and the consent must have a specific purpose. The consent must be:

- freely given
- specific
- informed
- unambiguous

In the case of a parent or carer giving consent for a child, every reasonable effort must be made to verify that the person giving consent does, in fact, hold parental responsibility for the child.

In all cases express consent must be obtained. Ways for consent to be withdrawn must also be supplied. St Francis will accept written instructions from individuals or their representatives wishing to withdraw particular consents for the school to process their personal data.

Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions. Jobs will bring the applicants into contact with children. The school has a duty under the Children Act 1989 and other enactments to ensure that all staff are suitable for the job. The school has a duty of care to all staff and students and must therefore make sure that employees and those who use school facilities do not pose a threat or danger to other users.

The school may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Privacy Notices

A privacy notice (previously called a fair processing notice) is available to pupils, their families, applicants for jobs and to staff at St Francis in order to meet the requirements of the 2018 General Data Protection Regulations. These can be found on our school website.

The notice outlines what information is collected, why it is held, and with whom it may be shared. The data can only be shared with the data subject (or their parents/carers in the case of children under 13 years old) unless the data subject has given permission for it to be shared.
Or
the law may also require that the information is shared. For a school these can be:

- School workforce census
- Pupil census
- information exchange when a pupil moves schools
- Exam entries and results

As well as the special reasons of:

- Protecting vulnerable individuals
- The prevention and detection of crime

Privacy notices are included in enrolment documentation, and are referenced at the end of any form that collects personal information such as:

- Application forms
- Admissions forms
- Data collection sheets
- Emergency contact forms
- Trips forms and permission slips
- Administration of medicine forms
- SEN documentation

They are distributed regularly via newsletters, the website, induction packs for new parents/carers or for new staff.

Details of any routine information sharing should be made known to those individuals concerned.

See below for St Francis Nursery and Primary School pupil and staff.

St Francis School and Nursery Privacy Notice Pupil Information

This Notice outlines how pupil information is processed and retained at St Francis School and Nursery.

The collection and use of pupil information

We collect and use pupil information under the 1998 Data Protection Act as well as Articles 6 and 9 of the EU General Data Protection Regulation which outline the 'lawfulness of processing'.

The lawful basis for personal information being processed by the School on behalf of Nursery is:

- That parents/carers have given consent for their child's personal data to be used when the child's place at Nursery is accepted

The lawful basis for the School processing pupil information is found in the following:

- The necessity to provide the legal and statutory education to children aged 4 to 11 years as mandated by the Government
- the performance of a task (education) necessary for public interest or in the exercise of any official authority of the controller

In addition, School and Nursery process particularly sensitive data about pupils such as ethnic origin and religion which is lawful because:

- a school must comply with a legal obligation to provide such data for census required by the DfE and Government

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to be able to provide targeted SEN support

The categories of pupil 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)
- School photographs
- Attendance information (such as sessions attended, number of absences)
- Information describing pupil assessments
- Relevant medical information (such as allergies) about conditions that may affect a child at school

Collecting pupil information

Whilst the majority of pupil information you, as parents and carers provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

At St Francis, this information is stored as paper records which are kept in a lockable room. The electronic files are stored securely on the St Francis server and on OneDrive.
The database supplied and managed by Capita called SIMs is used to manage the

electronic data and is subject to Capita's data protection provisions and retention guidelines.

We hold pupil data for certain periods of time, outlined in our Personal Data Management and Security Policy. The retention period for pupil personal files (electronic and paper) is generally the time spent at St Francis School. Paper records are forwarded to the education establishment a child goes to from St Francis. Remaining electronic records are either archived (if necessary) or deleted from pcs.

Other paper records such as registers of attendance; accident or serious incident forms; safeguarding incident reports have varying retention guidelines according to the sensitivity of the data. After the life of the record it is shredded securely in the main school office.

The sharing of pupil information
We routinely share pupil information with:

- The educational setting the pupil attends after leaving us
- Swindon Borough Council
- The Department for Education (DfE)
- The Diocese
- School nursing organisation
- The Police

All data is stored within the EEA (European Economic Area)

Why we share pupil information
We do not share information about our pupils with any organisation or individual without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements
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 DfE 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

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, or be given access to your child's educational record, contact the Office at St Francis School.

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

Every individual or parent/carer of a child below the age of 16 has the right to complain to the ICO (information Commissioner's Office) if unhappy with the way their personal data is being processed by St Francis School. The ICO can be contacted at https://ico.org.uk/concerns/handling
If you would like to see a copy of information about you that we hold, please contact the school office.

St Francis School and Nursery Privacy Notice Staff Information

for those employed to teach or otherwise engaged to work at St Francis School and Nursery

The Data Protection Act 1998 and GDPR 2018: How we use your information

St Francis Primary School and Nursery processes personal data relating to those we employ to work at, or otherwise engage to work at, our school. The lawful basis for processing this information is the fulfilment of an employment contract with the school, to allow individuals to be paid and to assist in the running of the school. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes:

- full name
- DOB
- address
- telephone numbers
- email address
- National Insurance number
- ethnic group
- religion
- employment contracts
- remuneration details
- qualifications
- absence information.

The information is stored as paper records which are kept in a lockable filing cabinet in a lockable cupboard in the School Office, which is also lockable. The electronic files are stored securely on the St Francis server and on OneDrive. The database supplied and managed by Capita called SIMs is used to manage the electronic data and is subject to Capita's data protection provisions and retention guidelines.

St Francis will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- Swindon Borough Council
- the Department for Education (DfE)

The retention period for staff personal files (electronic and paper) is seven years after the individual leaves St Francis after which time paper records are shredded and electronic records are deleted.

If you require more information about how St Francis and/or DfE store and use your personal data please visit:

- St Francis Primary School website for our policies
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Requesting access to your personal data
Under data protection legislation, every individual has the right to request access to information about them that we hold. To make a request for your personal information please contact the Office at St Francis School.

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

Every individual has the right to complain to the ICO (information Commissioner's Office) if unhappy with the way their personal data is being processed by St Francis School. The ICO can be contacted at https://ico.org.uk/concerns/handling

If you would like to see a copy of information about you that we hold, please contact the school office.

Processing Sensitive Information
Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the school is a safe place for everyone. Because this information is considered sensitive under the 1998 Act and GDPR, staff (and parents/carers of pupils where appropriate) will be asked to give their express consent for the school to process this data.

An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information
Certain items of information relating to school staff will be made available via searchable directories on the public web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school.

Personal and sensitive data
Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'personal data' is information which relates to a living, identifiable individual.

In the context of this document and the school's requirement to process 'personal data' as part of its duty of care and to educate its pupils, 'personal data' may include:

- school admission and attendance registers;
- a pupil's curricular records;
- reports to parents on the achievements of their children;
- records in connection with pupils entered for prescribed public examinations;
- staff records, including payroll records;
- pupil disciplinary records;
- personal information for teaching purposes;
- records of contractors and suppliers.

If it is necessary for the school to process certain personal data to fulfil its obligations to pupils and their parents or guardians, then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt (see below), will remain confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

Sensitive data may include:
- ethnic or racial origin
- political opinions
- religious beliefs
- other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- offence or alleged offence
- proceedings or court sentence

Where sensitive personal data is processed by the school, the explicit consent of the appropriate individual will be required in writing.

Under the 2018 GDPR, children are classed as 'vulnerable individuals' requiring special protection for their personal information. Being a primary school, St Francis will seek

authorisation from parents/carers for the processing of their children's data as a child under the age of 13 cannot legally give consent.

However, children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

Third parties

Where the school uses a third-party organisation and personal data is shared it is incumbent on St Francis to ensure that the 3rd party is compliant with the GDPR. Part of this means reviewing their data protection and security statements. (Copies of these can be found in the Personal Data Management and Security Policy).

When processing personal information shared by St Francis the 3rd party must:

- only act upon written instructions from St Francis
- ensure that their own staff are subject to a duty of confidentiality
- take appropriate measures to ensure the security of the data/processing
- not share the data any further
- allow subject access
- immediately alert the school to any data protection breaches
- delete or return all personal data at the end of the contract/agreed works

'Processing' can simply mean producing a list of participants and using it to schedule an event.

(See Personal Data Management and Security Policy for details of third party security/GDPR statements).

3rd Party Checklist

These are only the 3rd parties who have access to some of St Francis children's or staff personal data.

Contractors/other 3rd parties

3rd party name	Do we have a contract?	Have we checked DP compliance? How?	Date of check	Do we pass any personal data to this organisation? How does the org obtain the data?	Do we have their data security statement or equivalent?	Do we have their retention periods?	Notes
Edwards and Ward	Yes			No - but chef collects childrens' names and allergies from parents as well as parents email addresses			
Stone Group	Annual – email arrangements and all paperwork signed by St Francis Administrator	N/A	8.2.18	No - but data is on the equipment they are contracted to destroy	Disposal methods described in Certificate of Disposal	N/A	Certificates of disposal and log of what has been destroyed issued – kept by St Francis for six years
Parent Pay	Annual licence fee			Update link from SIMs			
Schoop		Yes	8.2.18	Parents sign up	Yes		
SIMs (Capita)	Yes			Yes via Redstor backups to their server		Being reviewed	
Target Tracker	Yes - annual			No – linked to SIMs			
CPoms							
NHS School Nursing Service	No			Yes – for care plans			
Butterflies							
Cool Milk				Parents sign up			
Parents evening system	Yes			Linked to SIMs			
Local Authority	Yes			Linked to SIMs Send us School Admissions forms			
Snappers school photographer	No – email arrangement		15/5/18	Yes, including images	Yes		
CLOUD	Microsoft Agreement			Storing information			

EasySchool	No			Host website			
Angel Solutions Perspectives							

External Clubs

3rd party name	Do we have a contract?	Have we checked DP compliance? How?	Date of check	Do we pass any personal data to this organisation? How does the org obtain the data?	Do we have their data security statement or equivalent?	Do we have their retention periods?	Notes
RPA Street Dance	No			School asks parents to book with org			
STFC	No			School asks parents to book with org			
Funrise	Yes			School asks parents to book with org			
RPA Performing Arts	No			School asks parents to book with org			
Soccer Excellence	No			School asks parents to book with org			
JS Academy Ballet	No			School asks parents to book with org			
Micro (Junior) Librarian							

Exemptions
Certain data is exempted from the provisions of the GDPR including:

- The prevention, investigation, detection or prosecution of a crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the school.

There are other exemptions under the act.

Retention of Data
The school has a duty to retain some staff and student personal data for a period of time following their departure from the school, mainly for legal reasons. Different categories of data will be retained for different periods of time. The time span can be requested in writing from school.

(see Personal Data Management and Security at St Francis Policy)

Data Protection Impact Assessment

Data protection impact assessments (DPIAs) help to identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy.

The GDPR (2018) sets out the circumstances in which a DPIA must be carried out.

What is a data protection impact assessment?

An effective DPIA will allow St Francis to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

A DPIA is carried out when:

- using new technologies; and
- the processing of the data is likely to result in a high risk to the rights and freedoms of individuals
- where there is large scale processing of special categories of data

At St Francis, a DPIA is also carried out when the personal data of a child is being collected and processed.

The DPIA contains:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

See DPIA form below.

The DPIA will be carried out by a member of the data protection team in consultation with the senior management team and Governors when necessary.
Should the DPIA assess the data processing to be in the 'major' impact category, and the risks cannot be addressed by St Francis, the ICO will be consulted.

St Francis Data Protection Impact Assessment Form

Impact assessment rated by the following:

- Major
- Medium
- Minor
- No impact

Completed by …….. Date ……..

Data asset	Purpose	How it is to be processed	Is processing in proportion to the purpose?	Risk to subject	How that risk is mitigated
IMPACT ASSESSMENT:					

Management of data protection breaches

This procedure outlines the process for detecting, reporting and investigating potential breaches of personal data.
There are different types of financial penalty for data breaches: fines for Personal Data Breaches (PDBs); and fines for Administrative breaches.
Data breaches can happen for a variety of reasons.

- Data loss scenario
    - loss or theft of data or equipment on which data is stored due to user error/system failure/natural disaster
- unauthorised access to and/or use of data, for example by a 'hacker'; misuse by St Francis if consent from the individual has not been obtained
- equipment failure
- human error
- unforeseen circumstances such as natural disasters
- 'blagging' – where data is obtained by an individual deceiving the school

Process
The St Francis Breach Management Procedure follows four steps:

- Containment and recovery
- Assessment of ongoing risk
- Notification of the breach
- Evaluation and response

Containment and recovery
Once a breach has been identified, the relevant members of the Data Protection Team should be alerted:

- Headteacher
- Administrative assistants with responsibility for Data Protection compliance
- Senior Management
- IT
- Governors

The lead person responsible for investigating the breach will depend upon the availability of that member of staff, and the type of breach that has occurred.
For instance, an IT breach may require system reviews and back up restores, whereas the theft of an emergency contact form from Reception could be mitigated in the future by better visitor vetting procedures.

Stage 1 – inform relevant staff
Stage 2 – attempt to recover the loss and limit the damage
Stage 3 – attempt to recover any equipment or restore data
Stage 4 – possibly inform the police

Assessment of ongoing risk
Some data security breaches result in inconvenience and can be solved relatively quickly and with little financial impact.
However, others can result in significant damage to the School's reputation, functioning and have serious cost implications.

(See St Francis Breach Risk Assessment Form below)

St Francis Breach Risk Assessment Form

Date ……..

Staff member making the risk assessment ……

Type of data involved	☐ Child/their family details ☐ SEN information ☐ Staff personal details ☐ Academic records ☐ …… ☐ Other (please state)
How is the data stored?	☐ Electronically ☐ Paper ☐ Other (please state)
How sensitive is the data?	☐ Serious eg personal or financial in nature ☐ Major ☐ Minor
What protections are in place to secure the data?	Please describe
What could happen to the data?	☐ Stolen ☐ Lost ☐ Damaged ☐ Transferred/transmitted to incorrect recipient ☐ ……

What could the data show about an individual?	Please describe
How many individuals' personal data could be affected by a breach?	
Who could be affected?	☐ Staff/volunteers ☐ Pupils ☐ Parents/carers ☐ ……..
What harm could come to those individuals?	☐ Physical safety compromised ☐ Damage to reputation ☐ Financial loss ☐ Identity fraud ☐ …… ☐ ……
Any wider consequences of a breach?	Eg. in the school itself, in the community

Notification of a data breach
In deciding whether or not to report a breach of data security consider:

- Who needs to be notified?
- What information do they need to be told?
    - A description of the breach and when it occurred
    - What data was involved
    - What is being done and will be done to respond to the breach
    - What can the individual do and how St Francis can help?
    - Provide a contact name and number for enquiries

- How will they be notified bearing in mind the security and immediacy of the communication method?
- How notification of the breach can be made to those concerned
- Should the LA to notified?
- Should the police be notified?

Escalating a breach to the ICO (Information Commissioner's Office)
Only when the breach may result in a risk to 'the rights and freedoms of individuals' should a breach be reported to the ICO.

There is a breach report form on the ICO website, or a call can be made to the ICO on 0303 123 1113 or 01625 545745.

Such a risk could include:

- Discrimination
- Damage to reputation
- Financial loss
- Loss of confidentiality
- Or other significant economic or social disadvantage

Where this risk is deemed high, those concerned should be informed directly and immediately of the breach.
The time limit for disclosing a relevant breach to the ICO is just 72 hours so it is important that an effective process is in place and staff are aware of it.

In escalating a breach to the ICO the following information should be provided:

- Where the breach occurred
- Who was affected
- What data was compromised
- The specific security measures in place when the breach occurred
- A copy of the risk assessment sheet
- Contact details of responsible staff member for managing the breach
- If the media is aware of the breach

Evaluation and response
Evaluating St Francis' response to a data breach can help to assess whether the data protection policies and procedures in place are efficient and appropriate. A 'de-brief' meeting should be held by the data protection team to establish any action arising from inadequate knowledge, processes or response from staff.

Data Protection Breach Register

Date of data security breach ……

Nature of breach ……

Where did the breach take place?	
Nature of data compromised?	
Who was affected and how?	
What security was in place?	
How was the breach handled? Who was informed?	 Individuals LA Police ICO Other
Any wider consequences for school?	
Was a risk assessment initially carried out and what level was the risk?	

Date of completion of this register ……

Staff member carrying out the entry …….

Conclusion

Compliance with the GDPR, which supersedes the 1998 Data Protection Act by enhancing the provision, is the responsibility of all members of the school. Parliament are considering a new Data Protection Bill based on the GDPR.
Any deliberate breach of this Data Protection Policy may lead to disciplinary action or even criminal prosecution.

Signed (Head Teacher) …….. Date ……..

Signed (Chair of Governors) …….. Date ……..