Saint Francis

St Francis Church of England Voluntary Aided Primary School

Personal Data Management and Security at St Francis

With regard to

The General Data Protection Regulation 2018

Version No	Date	Change/Review
V1.0	January 2018	Drafted
V1.1	May 15th 2018	Ratified
V1.2	Nov 2018	Review due
V1.3		

Contents

Introduction

Information records should be managed by school throughout their lifecycle, including electronic data such as email, to ensure that it becomes part of the vital record. All personal information must be managed in line with the GDPR and St Francis' Business Continuity Plan to ensure that records are secure, and are not lost or destroyed in the event of fire, flood or theft.

By efficiently managing records, St Francis will be able to comply with its legal and regulatory obligations.

This policy applies to all personal records created, received or maintained by staff of the school in the course of carrying out its functions. Personal records are defined as all those documents which contain details of pupils, their families/carers, external contractors, staff and Governors. These records may be created, received or maintained in hard copy or electronically.

Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the education system. The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access.

Pupils have a right of access to their educational record and so do their parents under the Education (Pupil Information) (England) Regulations 2005. Under the GDPR a pupil or their nominated representative has a right to see information held about them. This right exists until the file is destroyed. Therefore, it is important that all information should be accurately recorded, objective in nature and expressed in a professional manner.

The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of his/her school career. Key elements of the record include:

- Pupil's name
- DOB
- address
- name of the pupil's doctor
- emergency contact details
- gender
- preferred name
- ethnic origin
- language of home
- religion
- any allergies or other medical conditions that it is important to be aware of
- names of adults who hold parental responsibility with home address and telephone number (and any additional relevant carers and their relationship to the child)
- name of the school, admission number and the date of admission and the date of leaving
- UPN (Unique Pupil Number identifies each pupil in England uniquely. It is intended to remain with the child throughout their school career regardless of any change in school or Local Authority)
- parental permissions

At St Francis School, a database called SIMS is used to create, store and manage the pupil record.

SEN reports, child protection reports, Annual reports, certain information pertaining to children's needs, correspondence with external agencies and complaints from parents are filed in hard folders, or are stored electronically.

The following are also stored in hard folders: absence notes, parental consent forms for trips/outings, correspondence with parents about minor issues, accident forms, administration of medicines forms.

All pupil records are kept secure at all times. Paper records, for example, are kept in lockable storage areas or rooms with restricted access. Equally, electronic records have appropriate security such as password access only, auto-locks on pcs, and regular back-ups.

Access arrangements for pupil records at St Francis ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

Transferring the pupil record to the secondary school

St Francis uses SIMs to electronically transfer personal information about a pupil via a CTFile to the secondary school. Primary schools are not required to retain copies of any pupil records unless there is legal action underway when the pupil leaves. Files are not sent through the post, unless a pupil has moved out of area. Files delivered by hand are registered and signed for by the recipient using the Transfer of Records Log Sheet (Appendix A).

Staff Records

Applications for roles at St Francis are always retained as paper copies. Only once an individual has been appointed is their personal information stored electronically. Unsuccessful applications are retained for one year.

On leaving the school, the staff member's details are retained for five years and are then destroyed or deleted.

Swindon Borough Council also keep records of staff appointments.

Any personal data that is transferred externally to St Francis is logged on our 'Transfer of Information Log Sheet' (see Appendix A).

Retention Guidelines

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule for records created in the course of school business (see Appendix B for St Francis' Retention Schedule for Personal Data). Our Schedule for personal information is based on the IRMS retention guidelines for schools from 2016.

The retention schedule lays down the length of time which these record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule complies with normal processing under the GDPR and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored.

Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal relating to the request or legal hold must be stopped.

The school must not maintain and store information unnecessarily.

Closed School Guidance

Should a situation arise where St Francis School has to close, the following will happen to any personal information held:

- secure disposal
- secure storage for the life of the records - this would involve transfer to the Local Authority

Information Audit and Data Flow Analysis

All schools are designated 'Data Controllers' which means that St Francis retains overall responsibility for protecting personal data.

An information audit is a form of records survey encompassing the following:

- Paper documents and records
- Electronic documents and records
- Databases (proprietary or developed in-house)
- Microfilm/microfiche
- Sound recordings
- Video/photographic records (including those records taken on traditional magnetic tape and photographic paper but mainly digital sound, video and photo files)
- Hybrid files (paper and electronic information)
- Personal/individual knowledge

The information audit is designed to help organisations complete an information asset register and allows the school to identify the personal information it creates and stores. This facilitates correct management under the GDPR.

Information a school creates and uses to make the decisions which affect people's daily lives may well become subject to the Freedom of Information Act 2000.

An information audit collects the information necessary to formulate and implement an efficient records management programme and to ensure compliance with legislation.

See Appendix C for St Francis Information Audit Survey (to inform GDPR workbook)

See GDPR workbook for data flow.

Good Practice for Managing E-mail

As communicating by e-mail is quick and easy, e-mail discussions have largely replaced telephone conversations. However, information security still applies.

- E-mail is not always a secure medium to send confidential information. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a civil penalty of up to £500,000 from the Information Commissioner. Confidential or sensitive information is only sent by a secure encrypted e-mail system at St Francis. Personal information (such as a pupil's name) is never placed in the subject line of an e-mail
- All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Anything written in an email could potentially be made public. E-mails can remain in a system for a period of time after you have deleted them. Although the sender may have deleted their copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.
- E-mail can form a contractual obligation. Agreements entered into by e-mail can form a contract. Staff are aware of this if entering into an agreement with anyone, especially external contractors. Individual members of staff do not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.
- E-mail systems are commonly used to store information which should be stored somewhere else. All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files. Attachments containing any personal or sensitive data should be encrypted.
- Should it become necessary, St Francis School has a right to monitor the use and content of e-mail, provided it has obtained consent from members of staff that it may do so.

General rules relating to e-mail

- Does this transaction need to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.
- Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary.

- Never send on chain e-mails.
- When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.
- Be aware of 'phishing' and do not give out information without verifying the validity of the source of the request
- Always sign off with a name (and contact details).

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, a disclaimer covers the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school. There is some debate about how enforceable disclaimers are.

E-mail is primarily a communications tool, and e-mail applications are not designed for retaining emails as records. E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to content in the St Francis Retention Schedule (Appendix B). These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

Information Security and Business Continuity

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with the Data Protection Act 1998 and the 2018 GDPR. Taking measures to protect records can ensure that:

- school can demonstrate compliance with the law and avoid data loss incidents
- In the event of a major incident, school should be able to stay open and will at least have access to its key administrative and teaching records.

See St Francis' Business Continuity Plan for contingency arrangements.

All personal data is kept safe using secure measures appropriate to the data held. Measures in place include: secure passwords; a limit to the number of staff aware of the main server password (3); installation of firewalls and anti-virus software; the locking away of devices; and the shredding of hard copy confidential information.

Digital Information

In order to mitigate against the loss of electronic information:

- St Francis operates an effective back-up system which occurs every day, every week and every month to enable restoration of the data in the event of an environmental or data corruption incident. Back ups are kept for six months.
- The data is stored in the EU
- The South West Grid for Learning firewall adds a layer of protection

- Personal information is not stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff are advised not to hold personal information about pupils or other staff on mobile storage devices including but not limited to memory sticks, mobile 'phones, iPads, portable hard drives or even on CD.
- St Francis ensures that the data is subject to a robust password protection regime, with users regularly changing their passwords. PCs auto-lock when staff are away from their desk to prevent unauthorised use and require a password for re-entry
- Security updates occur automatically
- The server environment is managed to prevent access by unauthorised people.
- Restore processes are tested to ensure that the first time a problem is identified with a backup, it is not the first time the data needs to be retrieved

Specific systems used:

(see Appendix E for the 3rd Party GDPR/Security Statements

As well as the 3rd party checklist in our Data Protection Policy and GDPR workbook in Excel)

Capita SIMs

A folder only accessible to the nominated Data Protection Lead and Administrator is kept on the St Francis server in which to store reports from SIMs generated for Subject Access Request purposes.

SIMS backs up to the Cloud.

Links to Target Tracker (EES for schools) and CPoms

Parent Pay

tbc

Schoop

Schoop's data protection statement outlines that a school's personal information is only accessible to that school and is not shared with any other organisation. Any personally identifiable data collected via forms or surveys is encrypted in their database and can only be decrypted by Schoop software.

Website

The school website is created through Easy School.

CLOUD

Dropbox

Micro (Junior) Librarian.net

Records which are not stored on the school's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access.

- All vital information should be stored in filing cabinets, drawers or cupboards.
- Where possible vital records should not be left on open shelves or on desks
- Staff are encouraged not to take personal data on staff or students out of the school unless there is no other alternative. Records held within the school are in lockable cabinets.
- Access to offices in which personal information is being worked on or stored is restricted.
- All archive or records storage areas are lockable and have restricted access.

Disclosure

- Staff should be made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it.
- If personal information is shared with a third party, the requirements of the GDPR must be considered.
- Be careful of giving out personal information over the telephone; invite the caller to put the request in writing, supplying a return address which can be verified.

See St Francis' Data Protection Policy for our procedure in the event of a breach of personal information.

Disposal

The fifth data protection principle states that 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'.

Safe destruction of records

All records containing personal information should be made either unreadable or un-reconstructable

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records should be disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction (Stone Group). Staff working for the external provider should have been trained in the handling of confidential documents.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

The Freedom of Information Act 2000 requires schools to maintain a list of records which have been destroyed and who authorised their destruction. The following should be recorded:

- File reference (or other unique identifier)
- File title (or brief description)
- Number of files and date range
- The name of the authorising officer
- Date action taken

Following this guidance will ensure that the school is compliant with the 2018 GDPR and the Freedom of Information Act 2000.

See St Francis' ICT Disposal Policy

See Appendix F for St Francis' Disposal of Records Log Sheet

Transferring Records

All information records transferred to another organisation are logged on a Transfer Sheet – see Appendix A.

Digital Continuity Statement

The long term preservation of digital records is more complex than the retention of physical records. Much electronic data needs to be retained for longer than 7 years. If this data is not retained in accessible formats school will be unable to defend any legal challenge which may arise.

Flash drives (also known as memory sticks) are not be used to store any records. This storage media is prone to corruption and can be easily lost or stolen.

See Appendix D – St Francis Digital Continuity Statement

Appendix A Log Sheet of Records transferred by St Francis School

Name of Organisation/Record Office receiving record
Date
Description of record
Signature of recipient
Name
Designation
Organisation
Signature of St Francis staff member transferring record
Name
Designation
Organisation: St Francis School

Please return to the School Office for retention.

APPENDIX B St Francis Retention Schedule

Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

Governors				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Gov meeting agendas	May be dealing with confidential information regarding individuals		One copy retained with master set of minutes. All others to be disposed of	Secure disposal (cross cut shredding/electronic disposal)
Gov meeting minutes	May be dealing with confidential information regarding individuals			
Reports to Governors	May relate to staff or pupils/families		Min 6 years unless the report refers directly to an individual then it should be kept permanently	Secure Disposal or retain with minutes
Complaints	May relate to staff or pupils/families		Date of resolution plus min 6 years, then review for further retention in contentious disputes	Secure disposal

Head Teacher and Senior Management				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Minutes of SMT meetings/other internal meetings	May relate to individuals		Date of meeting plus 3 years then review	Secure disposal
Reports created by Head Teacher/SMT	May relate to individuals		Date of meeting plus 3 years then review	Secure disposal
Records created by any staff	May relate to individuals		Current academic year plus 6 years then review	Secure disposal
Correspondence created by any staff	May relate to individuals		Date of correspondence plus 3 years then review	Secure disposal
Professional development plans	May relate to individuals		Life of plan plus 6 years	Secure disposal

Admissions				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Nursery Admission applications	Relates to a child and family/carers		Date of addition to SIMS plus 3 years	Permanent records in SIMS
Any paperwork relating to admission information, including application forms/SIFs/birth certificate copies	Relates to a child and family/carers		Date of creation plus 3 years	Secure disposal
If the Reception/School admission (LA) is successful	Relates to a child and family/carers		Date of admission plus 1 year	Permanent records in SIMS
Paperwork relating to an Appeal	Relates to a child and family/carers		Resolution of case plus 1 year	Secure disposal

Operational administration				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Visitors' book and late sheets	Relate to personal information		Current year plus 6 years then review	Secure disposal
FAITH	Relate to personal information		tbc	
Newsletters/circulars that mention specific children, including Golden Book	Relate to personal information		Current year plus 1 year	Standard disposal
Text 2 parents				
Schoop				
SIMS				
Target Tracker				

Human resources

Recruitment/staff management				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
All records leading up to the recruitment of a new Head Teacher	Yes		Date of appointment plus 6 years	Secure disposal

Staff recruitment – unsuccessful candidates	Yes		Date of appointment of successful candidate plus 6 months	Secure disposal
Staff recruitment – successful candidates	Yes		All relevant information should be added to the personal file and other information retained for 6 months	Secure disposal
DBS checks			School does not have to keep copies of DBS certificates. Should there be any hard copies, they must not be retained for longer than 6 months	
Proofs of identity	Yes		These should be checked and a note kept of what was seen/checked. If a copy is kept this should be placed in the member of staff's personal file	
Evidence proving the right to work in the UK	Yes	An employer's guide to right to work checks (HO May 2015)	Add documents to personal file/or keep until termination of employment plus not less than 2 years	
Staff personal file	Yes	Limitation Act 1980 section 2	Termination of employment plus 6 years	Secure disposal
Timesheets/ Absence forms	Yes		Current year plus 6 years	Secure disposal
Appraisals	Yes		Current year plus 5 years	Secure disposal

Management of Disciplinary and Grievance Processes				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Allegation of a child protection nature against a member of staff where the allegation is unfounded	yes	"Keeping children safe in education March 2015"; "Working together to safeguard children. March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	Secure disposal
Disciplinary proceedings – verbal and first written warnings	Yes		Date of warning plus 6 months	Secure disposal
Further written warnings	Yes		Date of warning plus 12 months	Secure disposal
Final warning	Yes		Date of warning plus 18 months	Secure disposal
Disciplinary unfounded	Yes			Dispose at conclusion of case (unless CP related)

Health and Safety				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Records relating to accident/injury at work	Yes		Date of incident plus 12 years. In the case of serious accidents a further period will need to be applied	Secure disposal
Accident reporting	Yes		Adults – date of incident plus 6 years Child – DOB plus 25 years	Secure disposal

Payroll and Pensions				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**

Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year plus 3 years	Secure disposal
Pension information	Yes			

Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals.

Finance				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Pupil Premium	Yes			
Parentpay	Yes			
Free school meals	Yes		Current year plus 6 years	Secure disposal
Cool milk	Yes			
3rd party contracts Edwards and Ward Ian Reade Grounds/maintenance				

Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

Educational record/Attendance				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Pupil's educational record	Yes	The Education (Pupil Information) (England) Regulations 2005	Whilst pupil is at St Francis	The file will follow the pupil to secondary school/or transfer to another primary school. If the pupil dies whilst at primary school the file information should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home

				schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period.
Exam results	Yes		Add to pupil file	
SATs records	Yes		Current year + 6 years	Secure disposal
Child protection information held on Pupil file	Yes	“Keeping children safe in education March 2015”; “Working together to safeguard children. March 2015”	Should be in sealed envelope and retained for same period as the pupil file	Secure disposal - SHRED
Child protection information held in separate file	Yes	“Keeping children safe in education March 2015”; “Working together to safeguard children. March 2015”	DOB of child plus 25 years then review (sometimes by LA)	Secure disposal - SHRED
Attendance	Yes		SIMs Hard copies – date of entry plus 3 years	Secure disposal
Liaison with LA ref SIMs data	Yes			
Correspondence relating to authorised absence	Yes	Education Act 1996 Section 7	Current academic year plus 2 years	Secure disposal
Copies of referrals for Fixed Penalties	Yes			Secure disposal
Sick notes, medical evidence	Yes			
Emergency contact forms	Yes			
Data Collection Sheets	Yes			
Administration of medication/asthma inhalers forms	Yes			
Individual care plans	Yes			
Permissions/applications for trips	Yes		Conclusion of the trip	Unless major incident then all permissions to be kept for 25 years
School photographs	Yes		1 academic year	Some may be archived

Special Educational Needs

SEN Information				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
SEN referral	Yes			
Files, reviews, notes of meetings eg. TAC about a child	Yes		DOB of pupil plus 25 years	Review
EHCP	Yes		DOB of pupil plus 25 years	Secure disposal unless document is subject to a legal hold
Advice to parents	Yes		DOB of pupil plus 25 years	Secure disposal unless document is subject to a legal hold

Curriculum Management

Statistics				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Target tracker				
Exam results (school)	Yes		Current year plus 3 years	Secure disposal
SATs records	yes		Current year plus 6 years within school	Secure disposal
Pupils' homework	possibly			

Extra Curricular Activities

Activities Outside School				
File description	**Data protection issue?**	**Statutory Provision**	**Retention Period**	**Action at the end of the administrative life of the record**
Trips – consent forms where there has been no major incident	Yes		Until the conclusion of the trip	
Trips – consent forms where there has been a major incident	Yes		DOB of pupil plus 25 years (retain all slips for all pupils)	

Appendix C Information Audit Survey Form

St Francis Primary School	Department	Staff member providing information
Information Asset	Purpose and legal basis for collecting the asset	
Asset format Paper □ Electronic □ Other (specify) ………………...	If electronic, please tick form: Hard drive □ Server □ Cloud □ Email □ CD □ Tape cassette □ Floppy disk □	How many individual records are in the asset?
How is the asset stored?		
Who else accesses the asset?	How often is the asset accessed by the primary user? Less than once a month □ Once a month □ Once a week □ Every day □	
Retention period? Up to 1 year □ 1-2 years □ 2-6 years □ 6-10 years □ 10-25 years □	25-50 years □ 50-100 years □ archive □	Does a duplicate exist? If yes, where and in what form?
Assessment of risk should loss of this asset occur: Insignificant □ Minor □ Moderate □ Significant □ Major □		

Appendix D - St Francis Digital Continuity Statement

To be reviewed every two years in order to keep pace with advances in technology.

'An information asset is a body of information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and life cycles.'

At St Francis, all personal information assets are protected using backups and passwords as well as the SWGFL firewall, and have a clear purpose for being held. Our Retention Schedule identifies how long certain records can be retained and how such records should be disposed of securely (Appendix B).

Personal data is held by school in order to manage staff and human resource activities, pupils, and other adults working in the school. This information is also used for health and safety reasons, performance management and extra-curricular activities. See St Francis' Data Protection Policy.

The administrative team at St Francis have responsibility for long-term data preservation, along with the IT Manager and the Headteacher. The data held for long term preservation must be accessible when required but also must be protected against the standard information security requirements which are laid down for records within the authority. Governors hold ultimate responsibility for data protection infringements.

Where it is not possible for the data created by a bespoke computer system such as SIMs to be converted to the supported file formats, the system itself will need to be preserved.

All St Francis data is stored within Europe.

Appropriate Storage for Physical Records

Records are stored in school in a way that does not cause a health and safety hazard. Where appropriate, there are smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area is secured against intruders and has controlled access as far as possible.

The following are hazards which need to be considered before approving areas where physical records can be stored. At St Francis:

- Environmental Damage
  - Records can be damaged beyond repair by **fire**. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired. Core records are kept in lockable cupboards. Records which are stored on desks or in cupboards which do not have doors will suffer more damage than those which are stored in cupboards/cabinets which have close fitting doors.
  - Records damaged by **water** can usually be repaired by a specialist document salvage company. Where flooding is involved the water may not always be clean and records could become contaminated as well as damaged. Records are not stored directly under water pipes or in places which are liable to flooding and are kept in cupboards

with tight fitting doors which provide protection from water ingress. Records stored on desks or in cupboards without close fitting doors will suffer serious water damage.

- Records are not stored in direct **sunlight** (e.g. in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.
- Records are not stored in areas which are subject to **high levels of humidity**. Excess moisture in the air can result in mould forming on the records. The temperature in record storage areas should not exceed 18 degrees centigrade and the relative humidity should be between 45% and 65%.
- Records are not stored in areas which are subject to insect infestation or which have a rodent problem.

APPENDIX E 3rd Party GDPR/Security Statements

See hard copy folder:

Schoop

EES for schools Target Tracker

Micro Librarian

ParentPay

Angel Solutions Perspectives

Capita SIMS

Microsoft

Easy School (website)

CPoms

Snappers photography

Educare

APPENDIX F St Francis Disposal of Records Log Sheet

YEAR …………………….

File reference	Description	Information contained	Date range	Staff member managing disposal	Date and method of disposal