School Information Security Policy

St. Luke's Catholic Primary School

Approved by:	Governing Body	Date: Summer 2022
Last reviewed on:	May 2022	
Next review due by:	Summer 2023	

School Information Security Policy (SISP)
Version 6-22 Final

Contents

IMPORTANT NOTICE - ACCEPTANCE OF THIS DOCUMENT

This policy and all associated policies applies to all full time and part time employees, casuals, volunteers, temporary/agency staff, Governors of the school and all contracted third parties working for the school and partner employees, whether they are working on school premises or at any other premises, including their home.

Who should read this policy?

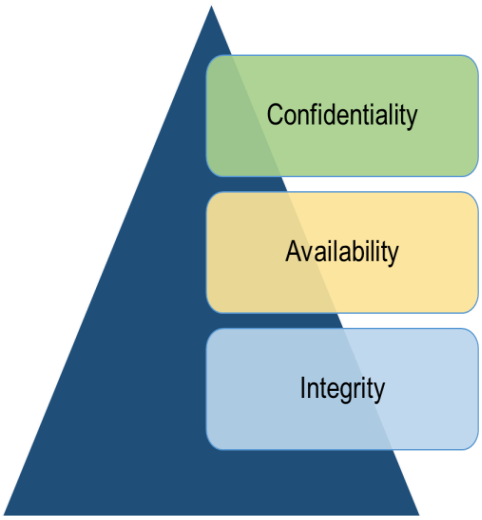
All school staff and Governors should read this policy

When you have read this policy document or the summary version, please indicate you have done by using the form at the end of this policy.

1. Introduction

1.1 Information can exist in many forms. It can be printed, written, stored electronically, transmitted by post, email, and fax or even spoken in conversations. The purpose of information security is to ensure that all information (including personal information) and associated processing systems are protected to an adequate level.

1.2 This policy sets out minimum standards and common acceptable use for confidentiality, integrity and availability of information to meet internal and legal requirements.



Ensuring that information is accessible only to those authorised to have access.

Ensuring that authorised employees have access to information when required.

Safeguarding accuracy and completeness of information and processing methods.

1.3 The policy has been written to conform, where possible, to standards such as ISO 27001 (Information Security Management standard), HMG Data Handling Guidelines, Government Functional Standard (GovS 007: Security) and PCI-DSS (Payment Card Industry – Data Security Standard).

2. Roles & Responsibilities

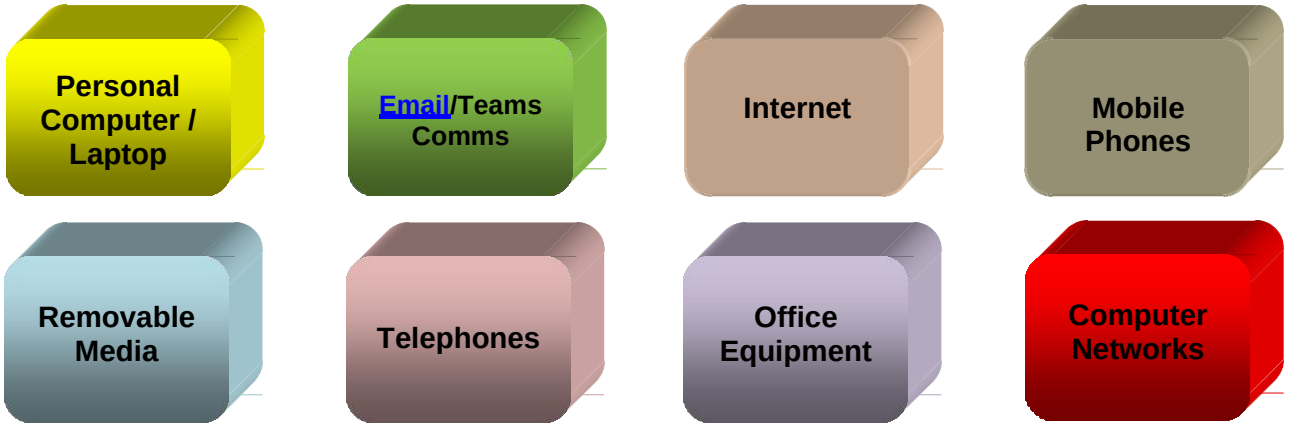
2.1 All employees within the school have a responsibility to ensure that they take steps to safeguard the security of the information that they are using and seeing.

All employees must:

- Read and comply with this policy (including linked acceptable use policies)
- Read and comply with the Information Security Breach Procedure (ISBP)
- Be personally responsible for work information held by them

3. Acceptable & Unacceptable Use

3.1 The school will not tolerate the use of any of its equipment/information for any purpose, which contravenes this policy and associated policies/documentation. Employees found not complying with these requirements might be subject to disciplinary action. This policy covers the following areas of use:



To view what is acceptable use and non-acceptable use for each of the categories above press the 'Ctrl' key and click on the relevant topic.

Employees should also ensure they are familiar with the requirements of other related policies on records management, data protection and social media.

4. Asset & Information Classification

4.1 In order to make sure that the School's information/assets receive an appropriate level of protection, all information will be treated in accordance with the requirements of ISO 27001 (Information Security Standard) and Government Security Classifications Policy.

5. Information Sharing

5.1 The schools Information Sharing Policy must be complied with at all times. Key points to note from this policy are that you should:

- Only share personal identifiable information (PII - Data about an individual that could, potentially identify that person) where there is legal justification to do so.
- Know the objective/reasons for sharing PII.
- Investigate whether the objective can be met without sharing PII.
- Only send the minimum PII needed to meet the objective/reasons.
- Where possible, anonymise the information you send so it is not personally identifiable
- Confirm the recipients contact details, e.g. postal address, email address, etc. before sharing information
- Appropriately protect the PII you are sharing by using a secure solution if it is electronic, sending post by special delivery/courier, etc.

5.2 The School will, where there is a defined justifiable purpose, sign up to information sharing agreements with partner organisations, where these agreements are within the boundaries of applicable legislation and regulation and do not compromise the School or the confidentiality of the personal and/or sensitive data that it holds.

5.3 The School will have put in place information sharing agreements where regular sharing of information from School systems/records takes place.

5.4 The Data Protection Officer has produced a standard data sharing agreement checklist and will advise and guide the school in developing data sharing agreements that cover specific requirements, suitable to their needs.

5.5 In order to ensure that information sharing takes place in an appropriate manner, all data sharing agreements should be approved by the Head Teacher.

5.6.1 Receiving and sending confidential/personal information

School staff have control over confidential/personal information they send to other parties. It is critical that appropriate security measures are in place before information is sent out. Staff have little control over how other organisations or the public may send confidential or personal information to the School. Staff must:

POST

Send information via special delivery, or if sensitive or a large number of personal details are included, use a reliable courier who will deliver to a named recipient only. Consider hand delivery if local, to someone known to you. Senders should be encouraged to send confidential/personal information to the School by special delivery/courier.

EMAIL

Only use secure email accounts

FAX

Only to be used in exceptional circumstances. Should send to a known fax number only and verify the number before sending. Ask if the fax is a safe haven (area that is secure and accessible only by authorised staff). If not request that the recipient stands and collects the fax as it is received. Also, discourage senders from using faxes.

6. Physical and Environmental Security

6.1 All employees have a responsibility for the physical security of School's assets (including information) including securing their laptops, locking away sensitive information, etc.

6.2 The school will be responsible for the provision of suitable physical, technical, procedural and environmental security controls in line with best practice such as ITIL (Information Technology Infrastructure Library – standard for IT service management) in order to prevent unauthorised access to, interference with, or damage to information.

6.3 Access Control

6.3.1 The management team have responsibility for authorising their staff to access information including IT networks, offices, secure filing cabinets etc. No School employee may access or attempt to access any information for which they have not been given authorisation.

6.3.2 The management team will remove access to information during periods of extended leave or sickness of more than 3 months. A review of employee's level of access to School information must be undertaken by their Manager during supervision.

6.3.3 Additional security measures shall be implemented by data owners to control access to especially personal/sensitive School data.

6.3.4 To control access to information, care must be taken (within the constraints of new ways of working) as to the physical positioning of desks and equipment used to view key personal, sensitive or confidential data. Desks used to process or view such data must be positioned away from doors/windows and public areas.

6.3.5 Managers must ensure appropriate access controls are in place for information processed in open plan offices. Adequate clear desk arrangements should be adhered to as outlined in this policy.

6.4 Physical security (equipment)

6.4.1 Desktop machines in public areas must be secured to protect against theft and/or unauthorised access.

6.4.2 Multi-functional devices (MFD) machines must be sited appropriately in areas where sensitive information can be handled.

6.4.3 Backup equipment and media must be sited at a safe distance to avoid damage from a disaster at the main site(s) and must be subject to the same environmental and physical protection as the main system.

6.5 Security of premises

6.5.1 Premises security consists of:

IDENTITY BADGES

All staff are issued with identity badges which include their photograph and these must be worn visibly at all times when working in/entering School buildings.

Staff must question anyone in any School building not wearing identification, where they are confident to do so. Staff must understand that they may be asked for identification at any time

Passes for visitors are controlled by Reception. Visitors to School offices must not be allowed to wander around the buildings and must be accompanied at all times. They must sign in and out at Reception and wear identification badges visibly at all times when progressing beyond public areas.

SECURITY PASS/FOB

Access to School premises is controlled by the issue of security passes or FOB's. Lleavers swipe cards / FOBs must be deactivated.

PHYSICAL ACCESS

Access to areas containing sensitive School information must be strictly controlled and given on a need to know basis. A record of privileged access granted to nominated individuals will be kept by the respective manager.

Physical security (door locks, locked cabinets, security card access) is the responsibility of all employees. Doors and windows must be locked as and when appropriate and blinds or curtains in place, with external protection considered for windows, particularly at ground and lower ground level.

7. Loss and/or Theft of Equipment, Files and Information

7.1 In the event of any loss/theft of equipment, files and information, the School's Information Security Breach Procedure should be followed. The key immediate actions include:

- Theft of equipment should be immediately reported to the police (obtain crime number) and to your SBM/Head and the schools ICT support. The SBM/Head will then inform the DPO.
- Theft/loss of files or information should be reported to the SBM/Head Teacherand DPO

8. Staff/User Access Management

8.1 Staff registration

8.1.1 The SBM/Head Teacher or Information Asset Owner must authorise access to information / systems for the provisional user with access being granted on a 'need to use' basis in order to carry out their duties. Access should not be granted prior to authorisation being given.

8.2 Password responsibilities

8.2.1 Good, secure passwords are essential and staff must be aware of what constitutes a suitable password. The School's Password Management Policy should be adhered to at all times.

Passwords must be:

- Changed regularly or immediately if there is any doubt at all that a password may have been compromised
- Kept confidential and never shared
- Changes at the first opportunity from default assigned passwords
- At least 12 characters long and complex, i.e. not be a simple word, name easily associated with you and contain numbers, a mixture of upper and lower case characters and allowed symbols

Passwords must NOT:

- Be easily guessable, and this includes dates of birth, family names, pet names, or other personal details
- Be shared with anyone else
- Be the same as your system user id
- Re-used on an alternate basis

Passwords should NOT

- Where possible be written down
- Where possible be duplicates of passwords used for other systems.

8.3 Leaving procedure

8.3.1 When staff leave the School, as part of the School's leavers procedure their manager is required to:

- Ensure that any information held in the leaver's homes drive (H drive) or One Drive, that is of importance to the School, is moved to a relevant network folder
- Request accounts to access systems to be deleted/disabled
- Ensure email accounts/contacts and membership of email group accounts are removed and, if appropriate, emails will be auto-responded to providing alternative contact details
- Ensure leaver returns all work ICT equipment/data

8.4 Non-electronic media

8.4.1 Paper media (including carbon copies, computer printouts, etc) containing information that is classified as personally identifiable or sensitive must be shredded on site. Disposal should be in line with the School's Information Retention Schedule.

8.5 Disposal of equipment

8.5.1 ICT equipment for disposal must be disposed of securely either by T&WC ICT or other reputable disposal company. ICT equipment no longer required must not be used by staff for personal use.

8.6 Third party access to systems

8.6.1 It is the responsibility of Information Asset Owners or SBM/Head Teacher in conjunction with ICT Technician to authorise third party access to resources and systems. User accounts and passwords will have to be created and where necessary relevant policies will have to be signed by the School and the third party prior to allow access.

8.6.2 It is the responsibility of the SBM/Head Teacher to advise the ICT Technician as soon as the third party access is no longer required.

8.7 Internet and intranet web publishing

8.7.1 Some staff will be authorised to publish data on the school website. This privilege must not be shared with staff who are not authorised to publish information.

8.7.2 The school is responsible for content which is published and must ensure that the information is correct, up to date and relevant and is published in plain English.

8.7.3 Inappropriate, illegal or offensive material must not be published. This will be removed immediately and may result in disciplinary action being taken against the offender.

9. Working from Home and Mobile Working Overview

9.1 There is a difference between “working from home” and “home working” and “mobile working”.

Working from Home	Home Working	Mobile Working
Work undertaken for limited periods but officer remains school based.	Officer’s normal place of work is their home and they do not visit the school daily.	Officer travels as part of their role and will require access to School facilities (network) whilst travelling.

Staff authorised as mobile workers or who may work from home **must**:

- Adhere to the School’s home working and remote working guidance documents
- only use School equipment to do their work unless accessing authorised cloud services
- ensure that all equipment and information is kept secure at all times, including ensuring that any equipment or information is not left “on show” in parked cars etc,
- only connect their School computers to any other non-School network using approved remote access technology. Personally owned ICT peripherals must not be connected to School computers connection
- never send any work information of any type to “non-work” email addresses
- never dispose of any used media off-site – it should be disposed of securely by ICT Technician

9.2 Staff are responsible for ensuring that unauthorised persons are not able to view confidential information or use School equipment. This includes family members and staff from other organisations.

9.3 Use of any confidential information at home must be for work purposes only. If the use of confidential information at home can be avoided, then the information should not be taken home.

9.4 Staff must ensure that when storing equipment/information at home, it is kept as secure as possible and if available is stored in a locked container.

10. Security Responsibilities for Staff and Delivery Units

10.1 SBM/Head Teachers must make it clear to their staff, where the job description is not explicit, the level of responsibility that they have for information that they handle. This includes compliance with key elements of this policy covering:

10.1.1 Password management – see section 8.2 of this policy and Password Management Policy.

10.1.2 Encryption and cryptographic controls - Appropriate encryption should be used to communicate / transfer data outside of the school.

10.1.3 System implementation and software purchase - all systems implementation and software purchases must be undertaken via the ICT Technician. Any projects that include the possible use of new computer systems/applications must engage ICT Technician prior to discussions with suppliers.

10.1.4 Clear screen and clear desk - Staff must ensure that they lock their PC screen when leaving their desk for a limited time, or log out when leaving for extended periods. School systems have an automatic lock out facility on PC's that do not need to be constantly logged on that will activate after several minutes of inactivity.

Desks and other spaces must be kept clear of any confidential information at all times when the information is not being used and you leave your desk for a short period and locked away out of sight after a longer period.

10.1.5 Human Resources employment checks - All appointments must comply with the Schools recruitment policy and include verification of an employee's identity, qualifications, employment history and eligibility to work in the UK.

10.1.6 Confidentiality agreements - As part of all employee's terms and conditions of employment, there is a requirement to maintain confidentiality of information both during and after their employment. Casual staff (including contractors/ agency staff) and third parties (including volunteers) not covered by an employment contract are required to sign a confidentiality agreement prior to being given access to information processing facilities. All such staff will be informed about the need to, and method for, maintaining confidentiality regardless of what access their role gives them to information.

10.1.7 Terms and conditions of employment - Employees of the School are expected to be aware of and comply with the all the codes of practice included within the Employee Code of Conduct, which includes responsibility for information security. Employees should also be aware that responsibility for information security continues beyond the end of their employment with the School and extends to all places and all times, including outside work. Breaches of confidentiality can lead to summary dismissal within the School's disciplinary procedure.

10.1.8 Training – All staff must ensure they complete relevant data protection training and keep up to date with information governance related policies and guidance.

11. Monitoring System Access, Use and Auditing

11.1 All School systems may be monitored to detect unauthorised activity or potential security breaches. Logged events may be reported and action taken if breaches or suspected breaches occur.

11.2 The School reserve the right to monitor, log, collect and analyse the content of all transmissions on networks/applications, including internet and email/Skype usage, at any time for system performance and fault diagnostic purposes as well as to detect unauthorised use of systems and to ensure that systems are being used in accordance with acceptable use policies.

11.3 Monitoring will be undertaken in accordance with legislation (Lawful Business Practices Regulations 2000 and Regulation of Investigatory Powers Act).

12. Communications and Operations Management

12.1 Employees must not:

- Copy materials (including newspapers) protected under copyright or patent law or make any materials available to others for copying. Employees are responsible for complying with copyright or patent law and applicable licences that may apply to software, files, graphics, documents, messages and other materials you wish to download or copy.

- Send, transmit or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to the School or any other organisation

12.2 Housekeeping

12.2.1 Managers should be aware of School equipment, information or software that is taken off site. In all cases, those personnel taking School assets off-site will be responsible for the security of such equipment/information at all times.

12.2.2 Individuals must be made aware that they may face disciplinary procedures that could lead to dismissal if found responsible for the theft of equipment, software or School information.

12.2.3 Staff handling personal/sensitive information must take extra measures, e.g. encryption, password protection, use of lockable storage, etc, to ensure information in their possession remains private and secure in order to comply with the UK Data Protection Act 2018.

12.2.4 The unnecessary processing of sensitive personal data in an identifiable form must be avoided. Managers are responsible for drawing up procedures for their area of work.

12.2.5 Documents and records must be stored under secure conditions up until the point that they are either destroyed/shredded at work or passed to a third party to carry out physical destruction. This means that they must not be left unsecured in skips, bins, reception areas, corridors etc.

12.2.6 Sensitive or confidential information must not be recorded on voice mail systems.

12.2.7 All employees should be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner must be obtained where documents are classified as 'highly confidential' or above.

12.3 Storage

12.3.1 The following requirements should be complied with:

- Compliance with the UK Data Protection Act 2018 for personal data storage
- Data maintained for a period that meets legal/business requirements as per the retention schedule
- Data stored is protected against loss and unauthorised/accidental changes

12.4 Audit trails

12.4.1 To protect both staff and the School, all systems have clear audit trails. This is particularly important for staff with administration rights.

12.5 Complying with legislation

12.5.1 Everyone has an obligation, under legislation such as Freedom of Information Act 2000 and UK Data Protection Act 2018, to deal with information in the stipulated way. Further guidance on this can be obtained from the Data Protection Officer.

12.5.2 It is the responsibility of the SBM/Head Teacher to make sure that staff are aware of any specific legislation applicable to their role including data protection.

13. Outsourcing

13.1 Any outsourcing must be with reputable companies that operate in accordance with quality standards. Such an undertaking must include a suitable Service Level Agreement (SLA), which meets the School's requirements. Where the processing of personal data is outsourced, a data processing agreement should be in place.

13.2 Where outsourcing includes the use of cloud computing the provider must provide assurance that cloud arrangements comply with recognised cloud security standards.

13.3 Any agreements or contracts must make it clear to the outsource organisation what their obligations are in respect of the UK Data Protection Act 2018 , Freedom of Information Act 2000 and other relevant information related legislation.

13.4 Outsourcing that may take place where information crosses outside UK and European borders must take into consideration the requirements of the UK Data Protection Act 2018 – the restriction of movement of personal data across boundaries outside the European Economic Area (EEA). This maybe particularly relevant to new technologies such as cloud computing.

14. Systems Development & Maintenance

14.1 Controls will be implemented to ensure that security requirements are considered when developing existing information systems and prior to introducing new ones.

14.2 Information governance (IG) requirements of systems

14.2.1 The Data Protection Officer will be involved in the development of new information system functionality (including new systems and development to existing systems) and processes that include the processing of personal information to ensure that all governance requirements are included.

14.3 Data input

14.3.1 Line managers will have responsibility to ensure their staff are aware of processes and procedures relating to quality of data input in line with data quality policies / requirements.

14.4 Data output validation

14.4.1 Staff must undertake data quality checks on data output to ensure it is accurate/ up to date and complies with any policies on data quality.

14.5 Security/Privacy requirements within projects

14.5.1 Managers are required to undertake a risk assessment/Data Protection Impact Assessment to identify security/data protection requirements for new School systems that process personal information.

14.6 Test environments and test data

14.6.1 Any systems being tested, or developed and tested will be separated from live systems. Live data will not be used and on logging in, the user(s) will be informed that they are in a test environment. Where development of systems occurs via a third party, there will an expectation that all testing will be completed to the relevant ISO standard.

15. Business Continuity

15.1 The School has a process for management of business continuity across the School.

15.2 Continuity plans must be in place to ensure continued access to, and protection of, service critical information.

16. Legal, Regulatory and Contractual Compliance

16.1 To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and any security requirement, compliance with this policy is mandatory. Failure to comply with policy requirements will be viewed as a breach of security. Any such event may be the subject of investigation and possible further action in accordance with the Disciplinary Procedure.

16.2 All parts of the School will be subject to review to ensure compliance with this policy. The Data Protection Officer may commence an investigation when the conditions of use have or may have been broken. Dependent on the circumstances staff may not be informed of the investigation. Whilst the investigation is under way, the staff member or account concerned may have their access rights suspended or reduced. If this occurs, the staff member will be informed.

16.3 Intellectual property rights (IPR)

16.3.1 Intellectual property rights include, but may not be limited to copyright, design and patents and trademarks.

16.3.2 Staff will not load software, video and audio files onto School systems without authorisation from ICT and that authorisation will include checking that any IPR has not been broken by the use of the software.

16.3.3 Licences for systems will be adhered to including making sure that any restrictions in the number of users for a particular piece of software are complied with.

16.3.4 Copies of software and systems will not be made by staff unless authorised to do so by the licence holder and ICT Technician.

16.4 Management of records

16.4.1 Information such as financial records, employee records, customer records and any records that are publicly accountable will be kept in accordance with ISO15489 records management recommended retention periods detailed in the Schools Information Retention Schedule.

16.5 Data protection and personal information

16.5.1 All personal information managed by the School is covered by the UK Data Protection Act 2018. This provides legislation as to how personal information may be used, stored, processed and shared. It contains six principles that the School should conform to and also governs how information needs to be handled under certain circumstances.

16.6 Freedom of Information (FOI)

16.6.1 The FOI Act 2000 governs access to non-personal information in public organisations. Any request for information to any member of staff, in written form, could be a request under this legislation. Staff must respond to these requests if they can answer the question quickly (opening times of offices etc) – known as business as usual requests.

16.7 Environmental Information Regulations

16.7.1 The Environmental Information Regulations (2004) covers the provision of information that is environmental in nature.

17. Advice & Guidance

17.1 Advice on this policy can be sought from your Data Protection Officer.

Appendix A - Acceptance form

School Information Security Policy – Acceptance Form

School	
Full name	
Job title	
Contact telephone	

- I have read, understood, and agree to abide by the Schools Information Security Policy.
- I understand that this policy may change and that I will read any new versions when I am informed that they are available.
- I further understand that I must read, understand and agree to abide by the acceptable use policies and codes of practice that are relevant to me and that if I have any questions that I may ask our Data Protection Officer for assistance.

Signed_____ **Date** _____

Document Version Control

Version	Date	Author	Sent To	Comments
6-20	22/9/20	R Montgomery	Schools	Updated policy to reflect changes to good practice
6-22	27/4/22	R Montgomery	Schools	Updated policy to reflect changes to good practice