Title	ICT Security Policy
Owner	Operations Manager
Issue Date	November 2024
Reviewed By	Bob Darby
Approved By	Risk and Governance Committee
Approved Date	February 2019 March 2020 November 2024
Next Review Due	October 2025

1 Purpose

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of the Church's information. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies. It supports the 6 GDPR privacy principles, the 7 Caldicott principles and uses ISO27001 principles to manage information security.

This policy covers:

- Scope
- Information Security Principles
- Governance – outlining the roles and responsibilities
- Supporting specific information security policies – Technical Security, Operational Security and Security Management

2 Scope

The scope of this policy extends to:

- All information processed by the Church, especially:
    - Sensitive personal information
    - Safeguarding information
    - Staff records
    - Church work information and membership records
- All ASWW owned IT Systems used in support of the Church's operational activities to store, process and transmit information.
- All users of the Church's Information Systems and equipment. This includes, but is not limited to, staff, interns, volunteers, consultants, and contractors.
- All external companies that provide contracted information services for the Church.

3 Information Security Principles

The core information security principles are to protect the following information/data asset properties:

- Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.
- Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.
- Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.

4 Governance – Roles and Responsibilities

4.1 Parochial Church Council (PCC)

The PCC, the body of Trustees for the Church, is legally responsible for information security.

4.2 Operations Manager

The Operations Manager is accountable to the PCC for ensuring that cost-effective security and legal controls are implemented that are appropriately matched with identified risk. As such the Operations Manager is the Information Governance Lead for the Church, and is supported in this task by the SMT, other members of staff and external consultants

All Information Security risks shall be managed in accordance with the Church Risk Management Policy.

The Operations Manager, or appointed delegee(s), are responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes, and

- Leads on the provision of expert advice to the Church on all matters concerning:
  - information security, compliance with policies, setting standards and ensuring best practice
  - the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018, compliance, best practice and setting and maintaining standards
  - Individuals' right to access information held by the Church
- Ensures the operational effectiveness of security controls and processes
- Monitors and co-ordinates the operation of the Information Security Management System
- Monitors potential and actual security breaches with appropriate expert security resource
- Provides a central point of contact for information security and a central point of contact for the DPA both internally and with external stakeholders (including the Office of the Information Commissioner)

4.3 Senior Management Team (SMT)

All members of SMT are individually responsible for ensuring that this policy and information security principles are implemented, managed and maintained in their respective areas of responsibility. This includes:

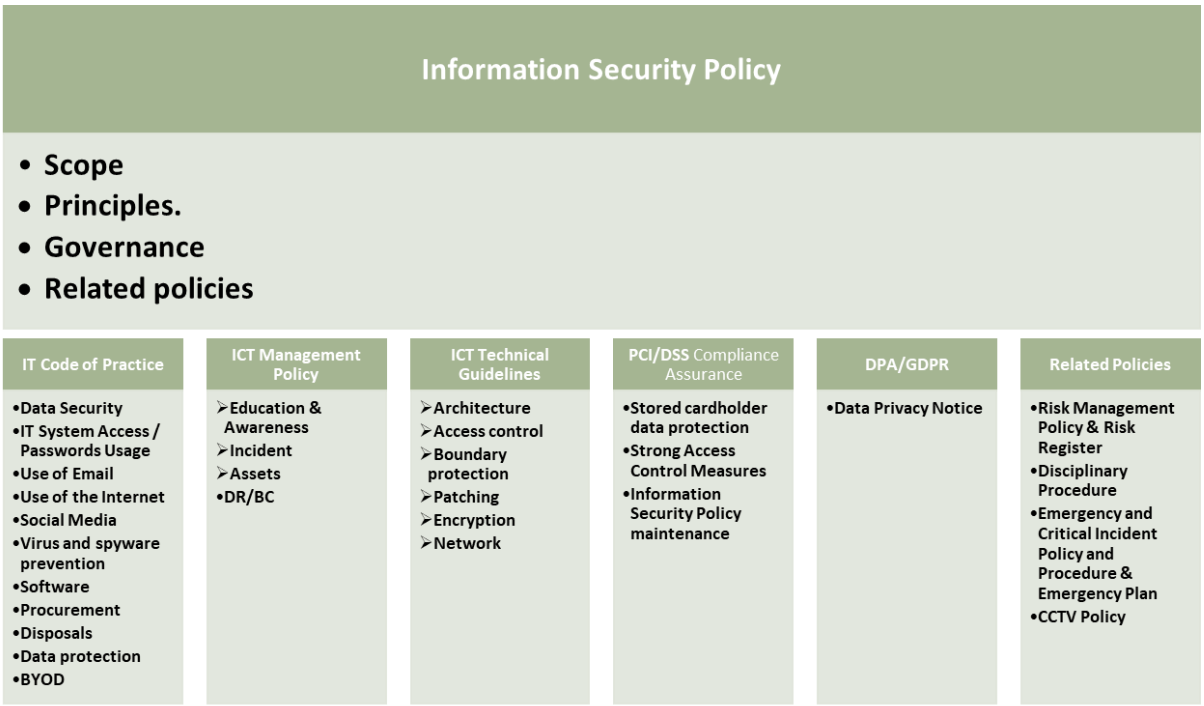
- Policy adherence by staff, interns and volunteers they are responsible for
- Awareness of information security risks, threats and possible vulnerabilities within their areas and complying with relevant policies and procedures to monitor and manage such risks
- Supporting personal accountability of users within their areas for Information Security
- Ensuring that all staff, interns and volunteers under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures

4.4 All Users (staff, interns, volunteers, consultants, and other individuals authorised to use Church Information facilities)

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are always expected to act in a professional and responsible manner whilst carrying out Church work. All users are responsible for information security and shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action.

5 Supporting Policies

The Information Security Policy is developed as a pinnacle document which has further policies, standards, guides and procedures which enforce and support the policy. The related and supporting policies are grouped into six areas as are shown in the following diagram.



5.1 IT Acceptable Use Policy

The purpose of the IT Acceptable Use Policy is to ensure computing resources, information and information processes are consistently protected according to approved security policy and practices, legal and regulatory requirements. It does this by defining acceptable usage of the Church's IT Systems. It is single document, written to be easily understood by all IT users. This IT Acceptable Use Policy must be followed by all users of the Church's IT systems. Agreement to comply with the practices laid out in the document is a pre-requisite to be granted access to the Church's IT systems.

5.2 ICT Management Policy

The ICT management policy details how security requirements are to be deployed, managed and checked. This includes general awareness and education requirements for users, interactions with third parties, how information security incident responses are to be handled, and how assets are to be managed.

5.3 ICT Technical Guidelines

The ICT Technical Guidelines policy details and explains how information security is to be implemented. It covers the security methodologies and approaches for elements such as ICT networks systems and servers, physical and environmental security, applications and desktops, patching, protective monitoring, secure configuration and legacy IT hardware and software.

5.4 PCI/DSS Compliance Assurance

The PCI DSS (Payment Card Industry – Data Security Standard) is a global standard, with compliance expected of any entity that stores, processes or transmits cardholder data.

The PCI/DSS compliance assurance document demonstrates that our handling of payments for goods via credit cards complies with requirements laid down by the credit card companies. The PCI DSS is not a legal requirement in UK law. However, credit card data is not just financial data but is personal data and comes under the GDPR and the DPA 2018. When the Information Commissioner looks at a breach of card data under his personal data remit, he will take account of whether the company was PCI DSS compliant. Specifically, the Information Commissioner's Office (ICO) advises that 'if online retailers do not adopt this standard or provide equivalent protection when processing customers' credit card details, they risk enforcement action from the ICO.'

5.5 Data Privacy Notice – Part of GDPR (General Data Protection Regulations)

The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data. The UK data protection regime is set out in the DPA 2018, along with the GDPR (which also forms part of UK law). The ICO regulates data protection in the UK.

A Data Privacy Notice (also sometimes referred to as a privacy policy) is a mandatory document required by the GDPR. It informs people how we collect, process and use their personal data, in plain and clear language, in an accessible format, and must be free of charge.

5.6 Related Policies

There are several other policies and related material that support overall Information security as detailed below:

1. Church Risk Management Policy & the Church Risk Register
2. Disciplinary Procedure
3. Emergency and Critical Incident Policy and Procedure & Emergency Plan
4. CCTV Policy

Appendix A: Caldicott Principles

The 7 Caldicott principles revised 2013 are:

Principle 1 - Justify the purpose(s) for using confidential information

> Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

> Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

> Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

> Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

> Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

> Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

> Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

Appendix B: DPA/GDPR Principles

To comply to DPA/GDPR, organisations broadly speaking need to embed seven privacy principles within their operations:

1. Lawful, fair and transparent processing – this principle emphasises transparency for all data subjects. When data is collected, it must be clear as to why that data is being collected and how the data will be used. Organisations also must be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the data protection officer is at that organisation or what data the organisation has about them, that information needs to be available
2. Purpose limitation – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place. Simply put, this principle says that organisations shouldn't collect any piece of data that doesn't have a specific purpose, and those who do can be out of compliance
3. Data minimisation – this principle instructs organisations to ensure the data they capture is adequate, relevant and limited. Organisations must be sure that they are only storing the minimum amount of data required for their purpose
4. Accurate and up-to-date processing – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organisation must have a process and policies in place to address how they will maintain the data they are processing and storing
5. Limitation of storage in the form that permits identification – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organisations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places. For example, organisations should prevent users from saving a copy of a customer list on a local laptop or moving the data to an external device such as a USB
6. Confidential and secure – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). An organisation that is collecting and processing data is now solely responsible for implementing appropriate security measures that are proportionate to risks and rights of individual data subjects. Organisations must spend an adequate amount of resources to protect data from those who are negligent or malicious. To achieve compliance, organisations should evaluate how well they are enforcing security policies, utilising dynamic access controls, verifying the identity of those accessing the data and protecting against malware/ransomware
7. Accountability and liability – this principle ensures that organisations can demonstrate compliance. Organisations must be able to demonstrate to the governing bodies that they have taken the necessary steps comparable to the risk their data subjects face. To ensure compliance, organisations must be sure that every step within the GDPR strategy is auditable and can be compiled as evidence quickly and efficiently. For example, GDPR requires organisations to respond to requests from data subjects regarding what data is available about them. The organisation must be able to promptly remove that data, if desired. Organisations not only need to have a process in place to manage the request, but also need to have a full audit trail to prove that they took the proper actions.