ALL SAINTS WOODFORD WELLS

Title	ICT Management Policy
Owner	Operations Manager
Issue Date	November 2024
Reviewed By	Bob Darby
Approved By	PCC
Approved Date	March 2019 March 2020 November 2024 March 2026
Next Review Due	March 2027

1 Purpose & Scope

The ICT Management Policy outlines the approach for managing, securing, and monitoring information systems within the Church. It ensures that information security is effectively deployed, managed, and audited. The policy also includes user education, incident response procedures, and asset management practices.

This policy covers the following areas:

- **Personal and sensitive data** processed by the Church, including:
    - Sensitive personal information (e.g., safeguarding data)
    - Staff records
    - Membership and church-related information
- **ASWW-owned IT systems** that store, process, and transmit information to support Church operations.
- **All users** of Church information systems and equipment, including staff, interns, volunteers, contractors, and consultants.
- **External service providers** contracted by the Church to deliver IT services or solutions.

This document is a part of the overarching Information Security Policy, approved by the PCC, and is authorized by the Operations Manager.

2 Governance – Roles and Responsibilities

2.1 Parochial Church Council (PCC)

The PCC, as the governing body of the Church, is legally responsible for the Church's information security strategy and ensuring compliance with relevant regulations.

2.2 Operations Manager

The Operations Manager is accountable for the overall management of ICT within the Church. The Operations Manager has specific responsibilities, including:

- Leading the Church's information security strategy, ensuring compliance with policies, and promoting best practices.
- Ensuring compliance with the **General Data Protection Regulation (GDPR)** and **Data Protection Act (DPA) 2018**.
- Overseeing access rights to Church-held information and ensuring adherence to privacy regulations.
- Ensuring effective security controls and processes are in place and monitored regularly.
- Coordinating the operation of the Church's Information Security Management System (ISMS).
- Monitoring and addressing potential and actual security incidents.

- Acting as the central point of contact for internal and external information security queries, including liaising with the **Information Commissioner's Office (ICO)**.

2.3 Senior Management Team (SMT)

Each member of the Senior Management Team (SMT) is responsible for ensuring that the ICT management policy is implemented and adhered to within their respective departments. Specific responsibilities include:

- Ensuring staff, interns, and volunteers under their supervision are aware of and adhere to this policy.
- Monitoring information security risks, identifying threats, and mitigating vulnerabilities within their area.
- Supporting personal accountability for information security within their teams.
- Ensuring staff have access to the necessary information systems required for their roles while maintaining security boundaries.

2.4 All Users

All individuals who use Church information systems (staff, volunteers, consultants, etc.) are responsible for the protection of information and assets. Users must:

- Understand and comply with the Church's information security policy and procedures.
- Act responsibly in managing Church information and IT systems.
- Be aware that failure to comply with this policy could lead to disciplinary action.

3 ICT Management

3.1 Education and Awareness

To ensure all users are aware of potential threats and know how to protect sensitive information, ICT security training will be provided. The training program will include:

- **Annual Training**: A review and update of training materials to address emerging security threats such as phishing and social engineering attacks.
- **Induction Training**: New staff, volunteers, and contractors will receive induction training on information security practices, including a review of the IT Acceptable Use Policy.
- **Ongoing Awareness**: Staff will be directed to additional training provided by software vendors or through online resources for specific systems.
- **Specialized Training**: Line managers are responsible for ensuring that staff receive any additional training specific to their roles or tasks.

The effectiveness of training will be monitored annually to ensure all staff and volunteers have up-to-date knowledge.

3.2 Incident Management

Operational incidents, including security breaches, are to be reported promptly. The process for managing incidents includes:

- **Routine Incidents**: Staff should report minor incidents via email or phone to IT support staff. These will be addressed within a reasonable time frame (typically weekly).
- **Urgent Incidents**: The Operations Manager will escalate critical incidents (e.g., security breaches or data loss) for immediate attention. The priority and escalation process will be determined based on the severity of the incident.
- **Third-party Engagement**: If third-party vendors are involved, interactions will be managed by IT support staff following the terms of existing contracts or service level agreements (SLAs). The Operations Manager will approve any additional expenditure related to incident recovery.

3.3 Asset Management

The Operations Manager is responsible for the management of all IT assets, including:

- Ensuring an **accurate asset register** is maintained.
- Overseeing the **acquisition and disposal** of IT equipment, ensuring that assets are securely disposed of or repurposed.
- **Auditing** IT assets on an annual basis to ensure that records are up to date and that assets are properly maintained.

3.4 Business Continuity / Disaster Recovery (BC/DR)

The Church's BC/DR policy is part of the broader **Risk Management Policy** and **Emergency Plans**. ICT-specific measures include:

- Backing up critical systems and data regularly to enable recovery in case of an incident.
- The Operations Manager, in coordination with IT support staff, will implement recovery measures in the event of an ICT-related disaster.
- The BC/DR procedures will be reviewed periodically to ensure that recovery times and business continuity can be achieved.

4 Security Measures

The Church employs various security measures to protect its ICT systems and data, including:

- **Encryption**: Sensitive data is encrypted both in transit and at rest.
- **Access Control**: User access to information is restricted based on role and responsibility. Each user is granted the minimum level of access required to perform their duties.
- **Firewall & Antivirus**: All systems are protected by up-to-date firewalls and antivirus software to prevent unauthorized access and protect against malware.

5 Monitoring and Compliance

The Operations Manager is responsible for ensuring compliance with this policy, as well as any relevant regulations such as GDPR. Regular audits of ICT systems will be conducted to assess:

- **Data Access**: Ensuring that only authorized users have access to sensitive information.
- **Incident Response**: Verifying that incidents are addressed promptly and in accordance with the policy.
- **Policy Adherence**: Monitoring compliance with training requirements and security practices.