INFORMATION SECURITY POLICY

PARISH OF HOLY TRINITY WITH ST COLUMBA FAREHAM

Introduction

This information security policy is a key component of the Parish management framework. It sets the requirements and responsibilities for maintaining the security of information within the Parish. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

1. Aim and Scope of this policy

The aims of this policy are to set out the rules governing the secure management of our information assets by:

- preserving the confidentiality, integrity and availability of our information
- ensuring that all members of staff and volunteers are aware of and fully comply with the relevant legislation as described in this and other policies
- ensuring an approach to security in which all members of staff fully understand their own responsibilities
- creating and maintaining within the organisation a level of awareness of the need for information
- detailing how to protect the information assets under our control
- This policy applies to all information/data, information systems, networks, applications, locations, staff and volunteers of the Parish or supplied under contract to it.

2. Responsibilities

- Ultimate responsibility for information security rests with the Parochial Church Council (PCC), but on a day-to-day basis our data manager shall be responsible for managing and implementing the policy and related procedures.
- Responsibility for maintaining this Policy, the Information Risk Register and for recommending appropriate risk management measures is held by the data manager. Both the Policy and the Risk Register shall be reviewed by the data manager at least annually.
- Line Managers are responsible for ensuring that their permanent staff, temporary staff, volunteers and contractors are aware of:
- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters
- All staff shall comply with the information security policy and must understand their responsibilities to protect the company’s data. Failure to do so may result in disciplinary action.

- Line Managers shall be individually responsible for the security of information within their area of responsibility.
- Each member of staff/volunteer shall be responsible for the operational security of the information systems they use.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contract shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

3. Legislation

- The Parish is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.
- The requirement to comply with legislation shall be devolved to employees, volunteers and agents of the Parish, who may be held personally accountable for any breaches of information security for which they are responsible.
- In particular, the Parish is required to comply with:
    - The Data Protection Act (1998)
    - The Data Protection (Processing of Sensitive Personal Data) Order 2000.
    - The Copyright, Designs and Patents Act (1988)
    - The Computer Misuse Act (1990)
    - The Health and Safety at Work Act (1974)
    - Human Rights Act (1998)
    - Regulation of Investigatory Powers Act (2000)

4. Personnel Security

Contracts of Employment

- Staff & volunteer security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff & volunteers shall be verified and a passport, driving license or other document shall be provided to confirm identity.
- Information security expectations of staff & volunteers shall be included within appropriate job definitions.
- Whenever a staff member leaves the company their accounts will be disabled the same day they leave.

Information Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
- Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff.
- An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved by the IT Manager. Individual and Parish intellectual property rights shall be protected at all times.
- Users breaching this requirement may be subject to disciplinary action.

5. Access Management

Physical Access

- Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.

Identity and passwords

- Passwords must offer an adequate level of security to protect systems and data.
- All passwords shall be ten characters or longer and contain at least two of the following: uppercase letters, lowercase letters and numbers.
- All passwords shall be changed if it is believed they have been compromised.
- Where available, two-factor authentication shall be used to provide additional security.
- All users shall use uniquely named user accounts. Generic user accounts that are used by more than one person or service shall not be used.

User Access

- Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a business need to access the information.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by the IT Manager.
- A list of individuals with administrator-level access shall be held by the IT Manager and shall be reviewed every 6 months

- Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

Application Access

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.
- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only.

System Perimeter access (firewalls)

- The boundary between church systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
- All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed if it is believed to have been compromised.
- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- The Parish reserves the right to monitor any systems or communications activity where it suspects that there has been a breach of policy, in accordance with the Regulation of Investigatory Powers Act (2000).

6. Asset Management

Asset Ownership

- Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

- An accurate record of Parish information assets, including source, ownership, modification and disposal shall be maintained.
- All data shall be securely wiped from all hardware before disposal.

Asset Handling

- The Parish shall identify particularly valuable or sensitive information assets through the use of data classification.
- All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.

Removable media

- Only Parish provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store church data and its use shall be recorded (e.g. serial number, date, issued to, returned).
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the IT Manager before they may be used on church systems. Such media must be scanned by anti-virus before being used.
- Where indicated by the risk assessment, systems shall be prevented from using removable media.
- Users breaching these requirements may be subject to disciplinary action.

Mobile working

- Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements
- Use of mobile devices for church purposes (whether parish-owned or personal devices) requires the approval of the IT Manager.
- Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.
- Users must inform the IT Manager immediately if the device is lost or stolen and church-owned information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

- Where necessary, staff may use personal mobile phones to access church email. This usage must be authorised by the IT Manager. The device must be registered in the asset records and must be configured to comply with the mobile working section and other relevant sections of this policy.
- No other personal devices are to be used to access church-owned information

Social Media

- Social media may only be used for church purposes by using official church social media accounts with authorisation from the IT Manager. Users of church social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.
- Church social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.
- Users shall behave responsibly while using any social media whether for church or personal use, bearing in mind that they directly or indirectly represent the Parish. If in doubt, consult the Rector.
- Users breaching this requirement may be subject to disciplinary action.

7. Physical and Environmental Management

- In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.
- Systems shall be protected from power loss by UPS if indicated by the risk assessment.
- Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

8. Computer and Network Management

Operations Management

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the IT Manager.

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the PCC.

Accreditation

- The organisation shall ensure that all new and modified information systems, applications and networks include security provisions.
- They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the PCC before they commence operation.

Software Management

- All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.

- All software security updates/patches shall be installed within 7 days of their release.
- Only software which has a valid business reason for its use shall be installed on devices used for church purposes.
- Users shall not install software or other active code on the devices containing church information without permission from the IT Manager.
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for church purposes.

Local Data Storage

- Data stored on the church premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).
- A backup copy shall be held in a different physical location to the church premises.
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

External Cloud Services

- Where data storage, applications or other services are provided by another organisation (e.g. a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

- The church shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
- All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system
- All anti-malware software shall be set to:
- scan files and data on the device on a daily basis.
- scan files on-access.
- automatically check for, and install, virus definitions and updates to the software itself on a daily basis.
- block access to malicious websites.

Vulnerability scanning

- The church shall have a yearly vulnerability scan of all external IP addresses carried out by a suitable external company.
- The church shall act on the recommendations of the external company following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities.

- The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

9. Response

Information security incidents

- All breaches of this policy and all other information security incidents shall be reported to the IT Manager.
- If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the IT Manager.
- Information security incidents shall be recorded in the Security Incident Log and investigated by the IT Manager to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Reporting

- The Information Security Officer shall keep the business informed of the information security status of the organisation by means of regular reports to the PCC.

Further Information

- Further information and guidance on this policy can be obtained from data manager Jim Palmer, who can be contacted on jim.palmer@htscf.org.uk Comments and suggestions to improve security are always welcome.

Agreed and paper copy signed August 2021