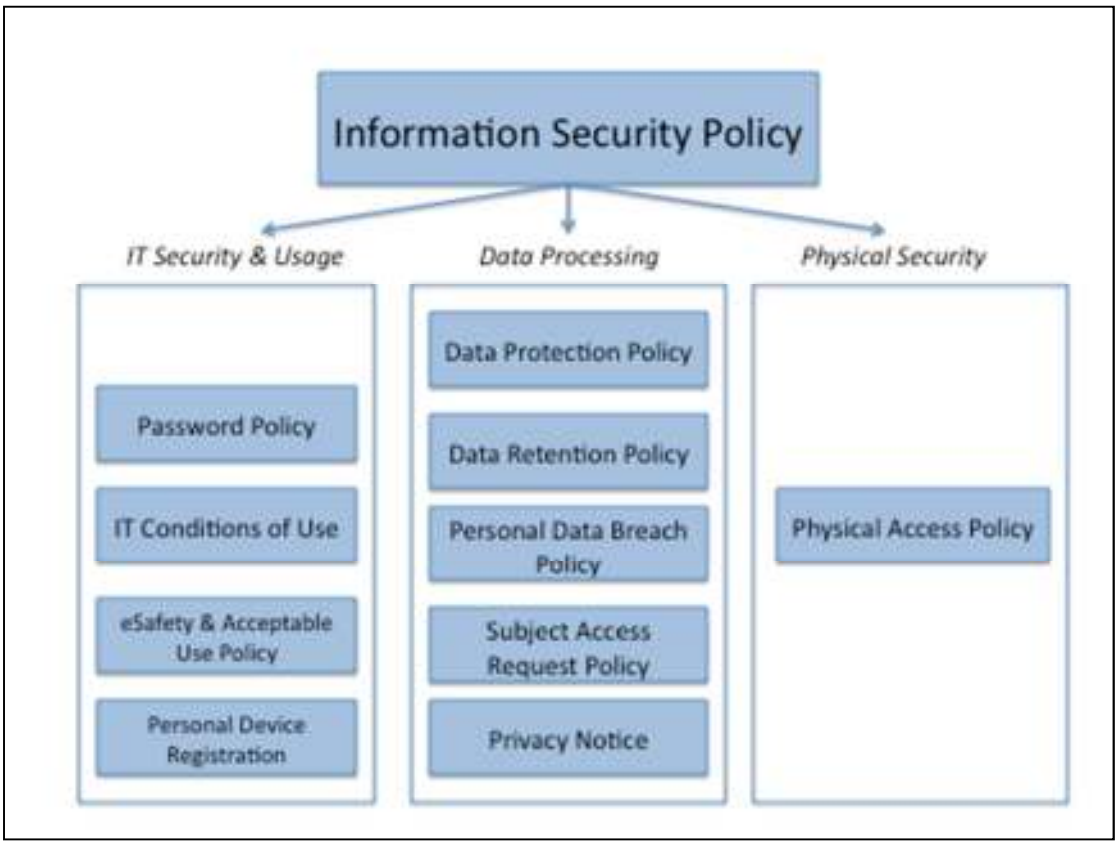
Youth for Christ Information Security Policy

1. Introduction

This policy sets out the overall information security management framework for Youth for Christ. The policy framework is as follows:



2. Objectives, Aim and Scope

2.1. Objectives

The objectives of Youth for Christ's Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and devices shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and devices owned or held by Youth for Christ by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all information, information systems, devices, applications and locations, trustees, staff and volunteers of Youth for Christ.

3. Responsibilities for Information Security

3.1. Ultimate responsibility for information security rests with the Trustees of Youth for Christ, but on a day-to-day basis the designated Data Protection Officer shall be responsible for managing and implementing the policy and related procedures.

3.2. The Data Protection Officer is responsible for ensuring that permanent and 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

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4. The Information Security Policy shall be maintained, reviewed and updated every three years.

3.5. Each member of staff and each volunteer shall be responsible for the operational security of the information systems they use.

3.6. 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.

3.7. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

4. Legislation

4.1. Youth for Christ is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Youth for Christ, who may be held personally accountable for any breaches of information security for which they may be held responsible. Youth for Christ shall comply with the following legislation and other legislation as appropriate:

- General Data Protection Regulation (GDPR) (2016)
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Privacy and Electronic Communications (EC Directive) Regulations (2003)
- 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
- Freedom of Information Act 2000
- Health & Social Care Act 2001

5. Policy Framework

5.1. Management of Security

- Responsibility for Information Security shall reside with the Data Protection Officer.
- The Data Protection Officer shall also be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.

- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

5.3. Contracts of Employment

- Staff contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions and induction.

5.4. Security Control of Assets

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

5.5. Access Controls

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

5.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.7. Computer Access Control

Access to computers shall be restricted to authorised users who have a business need to use them.

5.8. Application Access Control

Access to data 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 the availability of a licence from the supplier.

5.9. Equipment Security

In order to minimise loss of, or damage to, all assets and equipment shall be physically protected from threats.

5.10. Computer and Network Procedures

Management of computers and devices shall be controlled through standard documented procedures that have been authorised by the Trustees.

5.11. Information Risk Assessment

[The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence].

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.12. Data Classification

Youth for Christ has a data classification scheme to assist in managing security and risk:

Public Data:

Information intended for public use, or information which can be made public without any negative impact for the Youth for Christ

Internal Data:

Information regarding the day-to-day business operations of Youth for Christ. Primarily for staff, though some information may be useful to third parties who work with the organisation.

Confidential Data:

Information of a more sensitive nature for the business operations of the organisation, representing the basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role.

Highly confidential Data:

Information that, if released, will cause significant damage to Youth for Christ activities or reputation, or would lead to breach of the General Data Protection Regulations. Access to this information should be highly restricted.

5.13. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Data Protection Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.14. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Data Protection Officer. Users breaching this requirement may be subject to disciplinary action.

5.15. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Data Protection Officer before they may be used on Youth for Christ systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

5.16. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The Trustees audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above Act and the Human Rights Act

5.17. Accreditation of Information Systems

Youth for Christ shall ensure that all new information systems, applications and devices include a security plan (and in the case of devices a Personal Device Registration Form has been completed) and are approved by the Data Protection Officer before they commence operation.

5.18. System Change Control

Changes to information systems, applications or devices shall be reviewed and approved by the Data Protection Officer.

5.19. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Data Protection Officer. Users shall not install software on the organisation's property without permission. Users breaching this requirement may be subject to disciplinary action.

5.20. 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 devices.

5.21. Reporting

The Data Protection Officer shall keep the Trustees informed of the information security status of the organisation by means of regular reports.