1. Introduction

The organisation has a large investment in the use of Information Technology (IT) which is used to benefit all. In many areas of the work the use of IT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the IT systems and data are maintained at a level which is appropriate for our organisation's needs.

2. Policy Objectives

There are three main objectives of this policy:-

- To ensure that all our organisation's assets, staff, data and equipment are adequately protected on a cost-effective basis against any action that could adversely affect the IT services required to conduct our business.

- To ensure that staff are aware of and fully comply with all relevant legislation; and

- To create and maintain within all departments a level of awareness for the need for IT security to be an integral part of our day to day operation so that all staff understand the need for IT security and their own responsibilities.

3. Responsibility For Security

IT security is the responsibility of our organisation as a corporate entity and all members of staff.

The IT security policy will apply to all staff who use computer facilities whether they be mainframe, network or PC users. All members of staff are to be issued with computer security instructions which will specify their responsibilities and draw their attention to the penalties for not complying with the instructions.

All providers of IT services must ensure the security, integrity and availability of data within the service provided.

4. Legislation

The organisation has to abide with all UK legislation affecting IT. All employees must comply with the following Acts and they may be held personally responsible for any breach of current legislation as listed below and any future legislation that may be enacted:-

- Data Protection Act 1984

- Copyright Designs and Patents Act 1988

- Computer Misuse Act 1990

Information and guidance about the above Acts will be issued to all employees and agents.

5. Standards and Procedures

Physical Access

Precautions should be taken to ensure access to PCs is restricted at all times to authorised personnel.

Equipment should be sited to reduce the risk of damage, interference and authorised access.

All computer equipment must be security marked (with at least the organisation's post code) and be recorded on both the departmental inventories.

No equipment purchased, leased or hired may be connected to the network or attached to any equipment connected to the network without authorisation. This restriction also applies to any equipment not owned, leased or hired by the organisation.

Software Access

Terminals/PCs should not normally be left 'logged in' when unattended. Where this does occur it should be ensured that either a screensaver with password or time-out facilities are in operation.

Wherever the system allows, a screensaver providing immediate complete screen confidentiality should be used in conjunction with a password. This should be set to activate after a maximum duration of 10 minutes.

Passwords should be used to protect all systems and should not be written down or disclosed to others. Employees will be held liable for any misuse of a computer resulting from use of their password/username.

Passwords must be changed to a previously unused password several times each year dependant upon the sensitivity of the system. Passwords should be set wherever possible to automatically expire if not changed at a pre-determined frequency, e.g. log on to the network.

Proper mechanisms should be in place to notify system administrators of all leavers to facilitate the prompt removal of all access rights.

Passwords should normally be specific to individual staff and comprise a minimum of 6 alpha/numeric characters arranged in such a fashion as they will not be easily guessed.

Information

Information held on the organisation's IT facilities or subsequent output, e.g. printed letters/tabulations, is the property of the organisation and is governed by the provisions of the Data Protection Act. Any purpose for which personal information is held about people must be registered under the Act by the nominated Data Protection Officer.

Information held should only be released to authorised persons and IT facilities supplied must only be used for authorised purposes. Where IT facilities are used for personal work this activity must not prejudice or interfere in any way with the organisation's IT facilities or its business activities.

Any personal or sensitive data displayed upon unattended equipment must be protected, particularly in a public area, to ensure it may not be seen by anyone unauthorised to do so. This is applicable to information displayed on visual display units, printed output and computer produced media such as microfiche.

All computer output no longer required by the organisation should be disposed of with due regard to its sensitivity. Confidential output should be disposed of by shredding.

Any queries relating to the provisions of the Data Protection Act and how it affects your operations should be directed via your line manager to the head of IT Services.

Virus Protection

All PCs should be protected by virus detection software (obtainable from IT Services) which should be subject to regular updates to guard against new viruses. Any detected viruses must be reported immediately.

All USBs must be virus checked prior to use in any of the organisation's computers. This especially applies where disks have been received from an external source.

USBs must not be inserted into PCs until after the boot password has been entered and the computer has either reached:-

- The point where you log into the network, or
- The windows screen on stand alone computers.

Software Copyright

The copying of proprietary software programs or associated copyrighted documentation is prohibited and is an offence and could lead to personal criminal liability with the risk of a fine or imprisonment.

The loading of proprietary software programs for which a licence is required but not held is prohibited and this is also an offence which could lead to a large fine or imprisonment. All software system disks and licences should be held by the Parish Administrator

Personal software should not be loaded to organisation computers under any circumstances. If the software is deemed to be of use to the organisation then it should be duly acquired under licence.

Spot checks may be conducted by the Parish Administrator to ensure compliance with these provisions. The power to seek explanations from members of staff concerned and the right to remove any unauthorised software found to have been installed.

Computer Misuse

All employees should be aware of their access rights for any given hardware, software or data and should not experiment or attempt to access hardware, software or data for which they have no approval or need to conduct their duties.

Contingency Planning

Security copies (back-ups) should be taken at regular intervals dependant upon the importance and quantity of the data concerned.

In the case of stand alone computers, users should be aware that disks are susceptible to failure and should hold a copy of all data files on back-up media provided to all departments.

Security copies should be stored away from the system to which they relate in a restricted access fireproof location. Security copies should be regularly tested to ensure that they enable the system/relevant file to be re-loaded in an emergency.

Security copies should be clearly marked as to what they are and when they were taken. Depending upon the system concerned they should provide for system recovery at various different points in time over a period of several weeks.

Acquisition and Disposal of IT

All acquisitions should be in accordance with the provisions of the organisation's IT strategy and its financial regulations.

The disposal of personal or sensitive data must be arranged to ensure confidentiality.

Prior to the disposal of any PCs, all data should be permanently removed.

Disposals should be in accordance with the provisions of financial regulations which require the approval of the Parish Administrator for disposal procedures.

Suspected Security Incidents

It is the duty of all members of staff to report any suspected irregularities/fraud to their Parish Administrator as soon as possible. Such information shall be regarded as confidential by all employees involved.

6. Disciplinary Process

Computer security is viewed seriously by the organisation and any breach of this policy could lead to disciplinary action being taken against those who commit this breach. Mis-use of unauthorised software, the use of data for illicit purposes or the copying of software which breaches copyright agreements will be considered gross misconduct.