CUXTON PARISH COUNCIL
SERVING OUR COMMUNITY

Information Security Policy

INTRODUCTION

It is essential that all information processing systems within the authority are protected to an adequate level from disruption and loss of service, whether through accident or deliberate damage.

The document outlines the Council's policy in relation to the use of computers and especially the areas of:-

- Fraud
- Theft
- Use of unlicensed software
- Private work
- Hacking
- Sabotage
- Misuse of personal data
- Use of the Internet and email
- Disposal of Equipment

PURPOSE OF THE SECURITY POLICY

The purpose of the policy is to provide a set of rules, measures and procedures that determine the Council's commitment to ensuring that its I.T. (Information Technology) resources are protected from physical and logical risk.

The main objectives of the policy are:-

- To ensure that all the Council's assets, Staff, Councillors, data and equipment are adequately protected against any action that could adversely affect the I.T. services required to conduct the Council's business;
- To ensure that Staff and Councillors are aware and comply with all relevant legislation and Council policies related to how they conduct their day-to-day duties in relation to IT.

APPLICATION OF THE SECURITY POLICY

The policy is relevant to all I.T. services, irrespective of the equipment in use, or location, and applies to:

- All Councillors, employees and agents;
- Employees and agents of other organisations who directly or indirectly support or use the Council's ICT Services;
- All use of I.T. services within the Council.

MANAGEMENT OF THE I.T. POLICY

I.T. security is the responsibility of the Council, Councillors and all members of Staff. The Council approves the policy.

The policy has been reviewed by the Clerk in terms of the policy's scope, content and effectiveness. The Clerk will periodically review this policy.

The Authority will nominate an Information Security Officer whose responsibilities will include implementing, monitoring, documenting and communicating information security in compliance with the security policy and legislation.

Managers are responsible for ensuring that all staff are aware of their responsibilities under the policy and have access to the contents of this document.

The I.T. policy document is intended to be a living document, which will be updated, as and when necessary. Sections and appendices can be added to reflect new or amended procedures and guidelines when determined.

VIOLATIONS

Violations of this policy may include, but are not limited to, any act that:

- Exposes the Council to actual or potential monetary loss through the compromise of IT security;
- Involves the disclosure of confidential information or the unauthorised use of corporate data;
- Involves the use of data, which causes, for example, the law to be broken.

Any suspicion that this policy is being violated must be reported to the Clerk or Council Chair.

A log of all security incidents will be kept by the Clerk. The log is the responsibility of the Clerk. The log records any reported incidents and action taken.

Any breach of the security policy will be investigated and may result in the individual being subjected to the Council's disciplinary procedure. Councillor's breaches will be referred to the Council.

Internet use and access to web sites can be monitored. Any unacceptable use of this service may lead to disciplinary action against the individual concerned.

LEGISLATION COMPLIANCE

The Council has to comply with all UK legislation affecting I.T. All organisations, employees, Councillors and agents must comply with the following Acts and they may be held personally responsible for any breach of current legislation as listed below.

The following are brief descriptions on ‘key legislation’ affecting IT users. Do not assume that this covers all your legal responsibilities. If you are in any doubt about your legal responsibilities ask the Legal Section for assistance.

- **Data Protection Act 1994 & 1998**

  - Computers are in use throughout society – collating, storing, processing and distributing information. Much of the information is about people - 'personal data’. This is subject to the Data Protection Acts.
  - The Council is only allowed to record and use personal data if, under the Acts, there is a legitimate purpose for doing so and if details of the information, its use and source have been registered with the Data Commissioner. There are strict rules about how the information is used and to whom it is disclosed.
  - The Act gives rights to individuals about whom information is recorded on computer and in certain manual files. They may request copies of the information about themselves challenge it if appropriate and claim compensation in certain circumstances.
  - If there is any doubt about whether the information can be collected, used or disclosed please address queries to the Council’s designated Data Protection Officer.

- **Copyright Designs and Patent Act 1998**

  - Under this Act, any duplication of licensed software or associated documentation (e.g. manuals) without copyright owner’s permission is an infringement under copyright law. All proprietary software manuals are usually supplied under licence agreement, which limits the use of the products to specified machines and will limit copying to the creation of backup copies only. However in some instances, site licenses, permitting the use of software on all machines within a specified site are obtainable.
  - To combat the problems of illegal copying, software suppliers have formed their own organisation to police the use of software throughout the UK. The ‘Federation Against Software Theft’ (FAST) is able to conduct ‘spot’ checks on organisations, including local authorities, under a court order and without prior warning.
  - According to the Act, individuals found to be involved in the illegal reproduction of software may be subject to unlimited civil damages and to criminal penalties including fines and imprisonment.

- **Computer Misuse Act, 1990**

  - The Computer Misuse Act, 1990 was introduced to deal with three specific offences that were not adequately covered under existing laws:
  - Unauthorised access or attempt to access computer material (such as ‘hacking’). Under this offence it is not necessary to prove the users intent to cause harm;
  - Unauthorised access with intent. For example, hacking is carried out with the intention of committing a more serious crime such as fraud. Under this offence, if a plan has been hatched which involves the unathourised use of a computer, the unauthorised use will be sufficient to prove an attempt to commit the crime;

  - Unauthorised modification. This part of the act makes it an offence to intentionally cause unauthorised modification such as the introduction of viruses.
  - The intention of the act is to enable an organisation to take legal action to protect their data and equipment from unauthorised access and damage.

- **Health and Safety Act (1992)**

  - The Council shall ensure, through the appointed Health and Safety Officer that all IT equipment is located and used in such a way to not impede health of users or others.

- **Defamation**

  - Facts concerning individuals or organisations must be accurate and verifiable. Views or opinions must not portray their subjects in any way, which could damage their reputation.

- **Race Relations Act (1976) & Sex Discriminations Act (1976)**

  - Accessing or distributing material, which might cause offence to individuals or damage the Council's reputation, is forbidden. For example pornographic, racist or sexist material.

- **Criminal Justice and Public Order Act 1994, and Obscene Publications Act (1959 & 1964)**

  - To ensure this law is complied with, any use of Shrewsbury and Atcham Borough Council's computer equipment for viewing, reading, downloading, uploading, distributing, circulating or selling any material which is pornographic, obscene, racist, sexist, grossly offensive or violent is strictly forbidden. This is irrespective of laws regarding the material in the country of origin.

- **Human Rights Act 1998 (operative October 2000)**

  - Under this Act, everyone has a right to respect for their private life, their home and correspondence, which is commensurate with the need to protect the Council from fraud, introduction of viruses or breach of other overriding considerations. To this end, the Council reserves the right to monitor usage of PC's and telephones.
  - Individuals using the Internet, e-mail or telephone should respect the confidence of the Council and colleague's information in disclosing it to other people. E-mail, in particular, should not be circulated in a tone, which may give rise to a claim of inhuman or degrading treatments.

- **Freedom Of Information Act (2000)**

  - Any person making a request for information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the description specified in the request, and if that is the case, to have that information communicated to him.

- **Electronic Communication Act 2000**

  The main purpose of the Act is to help build confidence in electronic communications. The Act creates a legal framework for electronic commerce, It:

  - Clarifies the legal status of electronic signatures.
  - Gives the Government powers to modernise outdated legislation so that the option of electronic communication and storage can be offered as an alternative to paper.
  - Provides a fallback to self-regulatory scheme that will ensure the quality of electronic signature and other cryptography support services.

- **Regulatory Investigatory Powers Act 2000**

  - Interception of communications including computer communications such as email, are unlawful unless in accordance with the RIP Act 2000.
  - The Council may monitor and record communications for the following purposes:-
  - To establish facts and monitor performance of standards.
  - In the interests of national security.
  - To deter crime.
  - To detect unauthorised use of the system.
  - To secure a system.

ASSETS CLASSIFICATION AND CONTROL

The Authority positively identifies and keeps documentary evidence of all computer equipment. It is the responsibility of the Clerk to ensure that these records are accurate and continuously maintained.

Each inventory item must clearly identify each asset by an identity tag detailing its unique asset number.

All equipment is marked to identify ownership to Shrewsbury Borough Council.

The inventory is maintained using a database, including information relating to location, user, asset tag number, and serial number.

On receipt of new equipment it must be labeled and recorded on the inventory.

All disposals of equipment should be recorded against its original entry. The Authority actively pursues a ‘green policy’ on recycling IT equipment.

An annual audit of equipment should be carried out by all departments and accounted for to ICT Services.

No equipment should be relocated without prior consultation with the Clerk

PERSONNEL SECURITY

Security in Job Definition and Resourcing

The authority should ensure that there is adequate definition of responsibilities in Job descriptions for security responsibilities.

All Staff commencing employment with the Council agree to comply with this policy.

Personnel procedures ensure that all Staff are made aware of these policies during their 'induction process'.

Copies of the policy are available from the Clerk.

Training

Each new employee is made aware of his or her obligations for security during the Council's induction-training program. This includes Staff being told of the existence of the Security Policy.

Training requirements are reviewed on a regular basis to take account of the needs of the individual, and to ensure that staff are adequately trained in the use of technology.

PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY

Security of Equipment

Where possible Computer equipment is to be sited away from public areas. Where this is not possible the equipment is always supervised.

Computer screens and printed output should not be in view of unauthorised persons.
All computer screens that are in public areas should be controlled by time delayed screensavers which require a password to access information.

Staff should take responsibility for the physical security of their Computer Equipment within their working environment. Windows and doors should be kept shut whilst unattended.

Security of Equipment off-premises

Equipment used outside of the Authority is only to be used for work purposes.

Portable computers are very vulnerable to theft; loss and unathorised access when travelling. The high incidence of car theft makes it inadvisable to leave equipment or media in an unattended vehicle.

All portable computer equipment is to be insured with the Council's insurance provider.

Equipment Disposal

All items of equipment containing storage media are only disposed of after reliable precautions have been taken to destroy the media.

A record is maintained of all equipment recycled.

COMPUTER MANAGEMENT

Operational procedures

Backup and system procedures are kept of all fundamental systems, including:-

- General Operations of ICT Services.
- Day to Day operations and work schedules.
- Year-end procedures.
- Recovery procedures.

Protection from Malicious Software

The Council uses antivirus software as a means of protecting itself from malicious attack. All Servers and workstations are installed with up to date antivirus software.

The Clerk is to periodically check to ensure that all workstations and Servers are updated with the most up to date version of antivirus software available.

No Staff should load or install software on any Council computer without the prior consent of ICT Services.

No USB/Memory sticks should be loaded onto a Council workstation without them first being swept for viruses. No MP3 players should be connected to Council computers.

Data Backup/Media Storage

Back-up copies are taken of all essential data, software and system files weekly. The backup procedures ensure that all critical systems can be recovered in the event of a disaster.

Backups are checked weekly to ensure that they have completed.

All Backups are clearly labeled and after completion are removed off-site.

Media Data Handling Procedures

See also Data Backup procedures.

No data is removed for transportation unless it is signed for or collected by an authorised employee or Courier.

All data is packaged accordingly to protect it during transit.

Media Disposal

All magnetic data is destroyed if the equipment is to be disposed of. Where the equipment is to be recycled the magnetic data is reformatted or checked with specific software to clear the data. Where a third party Contractor is used to ‘clear data’ a legal disclaimer is required.

BUSINESS CONTINUITY PLANNING

Risks and Planning

The Clerk has identified business critical systems and processes.

The Clerk periodically reviews operational risks and their impact on the Council.

All Staff responsible for Recovery procedures will be trained accordingly.

Procedures are tested and reviewed regularly.