Starston Parish Council

Information and IT Security Policy

Overview

1. The policy covers employees and Councillors and self-employed persons and any persons acting on behalf of the Council. Plus, any users of Council information documents or IT equipment.
2. Individuals may have responsibilities both as an information owner and user.
3. Failure to comply with the provisions of the policy may result in legal or disciplinary action.
4. Information should not be protected beyond the value of the information.
5. Reasonable and appropriate care must be taken at all times with information that has been given by individuals for the purpose of undertaking the provision of Parish Council services.
6. No information should be left unprotected, particularly in locations with unguarded access such as public places.
7. External network access requires additional safeguards and vigilance.

Introduction

The Parish Council is becoming more dependent upon the use of Information Systems for its delivery of services; these include planning and administration. The Information and IT Security Policy communicates to everyone the principle that information is a valuable asset to the Council and that everyone is responsible and accountable for protecting it.

The policy encompasses all information whether stored electronically or manually. The Council operates through its information, which is its lifeblood. If any of this gets lost or destroyed whether by accident or by malicious intent then Council activities are likely to suffer.

All Council information should be classified into two categories: **A**. Information that is unique to the Council, eg Council's own financial records, deeds etc. **B**. Information that is not unique, eg Planning applications etc.

Information must be protected. For this to be complete, all Councillors and employees should be aware of the following basic components of information security:

1. Confidentiality – Protecting information from unauthorised disclosure or interception.
2. Integrity – Safeguarding the accuracy and completeness of information.

3. Availability – Ensuring that information is available to authorised users when required.

The Information and IT Security Policy describes what information must be protected, who must protect it, and how it must be protected. It states requirements for conduct and responsibilities and the consequences for misuse of information resources. In particular the policy outlines:

1. What information must be protected and what level.
2. Who is responsible for protecting information assets.

Objectives

The objectives of the policy are to ensure that:

1. Information is sufficiently protected from unauthorised access, disclosure, modification or loss.
2. Information and equipment are sufficiently protected from accidental or malicious damage.
3. Potential risks are identified, assessed and managed.
4. Audit records are created and maintained.
5. All statutory (including Data Protection Acts), regulatory, contractual and standard requirements are met.

Policy Obligations

Starston Parish Council accepts all obligations in respect of information security and the protection of information in its control by implementing recognised best practices that will achieve a balance between cost and risk.

Who and What are Covered by the Policy?

The policy applies to all information stored either electronically or by any other means. The policy will be reviewed from time to time by the Parish Council. Reviews should cover:

1. ICT systems and system providers (Parish Council property only)
2. Information and data owners (Parish Council property only)
3. All paper-based records
4. Users (including Councillors who subsequently retire or resign during the current Council term)

Information Owners

The owner of information (normally the Clerk to the Parish Council) is usually responsible for the creation and handling of this information. The owner is normally responsible for:

1. Knowing the information assets for which they are responsible
2. Specifying and ensuring effective controls and back-up
3. Periodically reviewing control decisions
4. Judging the value and importance of their information
5. Having responsibility for authorising access to all users
6. Communicating protection requirements to all users
7. Promptly reporting any misuse or losses (controlled by self-regulation)
8. Taking reasonable steps to understand conditions surrounding custody or use of the asset and initiate appropriate actions when problems are identified
9. User education and awareness
10. Understanding risks to information
11. Specifying special protection

The Chairperson

The Chairperson will be responsible for ensuring that information users are aware of the policy and that they comply with its procedures. The Chairperson should also set up a regular review of the policy with the Clerk and other Councillors.

Users

All users of Parish Council information systems have a responsibility to be aware of the Information and IT Security Policy and to ensure they adhere to it.

PERSONS AUTHORISED TO USE THE INFORMATION ARE:

1. All Councillors
2. The Clerk
3. Any Council Agent
4. Members of the public may obtain information via the Clerk (only to obtain public information)

Users of Information must:

1. be responsible for using the organisation's systems and information.
2. demonstrate awareness and use of current controls.

3. comply with the current policy.
4. promptly report any loss or misuse of information (controlled by self-regulation).
5. be authorised by owners to handle information.
6. Remote access to third party networks via the internet is only envisaged for the sending of emails and the gathering of relevant information, including downloading government documents.
7. All users are reminded of their obligation not to use the internet for illegal or offensive reasons.

Clerk's Accountability Issues

The Clerk will keep an inventory of assets that will be available for audit on the following:

Hardware Assets

1. Computer equipment
2. Communications equipment
3. Other technical equipment

Software Assets

1. Application software
2. System software
3. Virus protection system

Information On IT and Paper-Based Assets

1. Databases
2. Data files
3. System documentation
4. Document files

Housekeeping and Security Issues

1. It is the Clerk's responsibility to maintain the integrity and availability of services, good housekeeping practices and regular data back-up.

2. Back-up material should be kept in a secure place. Paper-based records should be stored in dry conditions. All files and back-up material over 5 years old should be stored at the County Records Office.
3. IT equipment should be installed in accordance with the manufacturers' instructions.
4. All equipment should be protected by appropriate insurance.
5. Portable equipment must not be left unattended.
6. All Council owned equipment should be protected by a suitable PASSWORD.

7. Data back-up should be kept for a minimum of at least 24 months.
8. To keep an adequate up-to-date virus protection system.
9. All paper-based files to be kept in an appropriate filing system.

Access to Systems and Data

Access is defined as:

1. Who is allowed to use the resources.
2. What is the proper use of the resources.
3. What services are approved.
4. Who is authorised to approve access and usage.
5. What are the users' rights and responsibilities.
6. All users must keep the virus protection system on when using the Council's computers.

Access Control

Access to data and equipment will be in accordance with the law and subject to approval by the Chairperson or Clerk. A log must be kept of **all users**.

User Responsibilities in Respect of Passwords shall be

1. Keep all passwords confidential.
2. Avoid keeping a written record.
3. Not use save password options.
4. Choose passwords of at least 6 characters.
5. Regularly change passwords.

Contingency Planning and Disaster Recovery

The information owner will have primary responsibility for the production of a business recovery/continuity plan. The Clerk will carry out a risk assessment into the potential loss of data and equipment. The risk assessment and continuity planning process should cover as a minimum:

1. A recovery and continuity plan

2. Documented procedures
3. Testing of plans
4. Regular updates

The Clerk will be responsible for ensuring all relevant licences are up to date and renewed accordingly.

This Information and IT Security Policy was approved at a meeting of Starston Parish Council

On 19th May 2025

Signed

Position on the Council – Chair

Date of next review – May 2028