Silverdale Parish Council - Information Security Policy

ADOPTED JUNE 2019

1. Introduction

The continued confidentiality, integrity and availability of information systems underpin the operations of the Parish Council. A failure to secure information systems would jeopardise the ability of the Council to fulfil its responsibilities and have greater long term impact through the consequential risk of financial or reputational loss.

This policy provides the guiding principles and responsibilities of all members of the Council required to safeguard its information systems.

The Information Security Policy applies to **all forms of information**, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by, administered or controlled by the Parish Council, including information, which is:

- Spoken face to face, communicated by fixed line, by mobile telephone, or by two-way radio
- Written on paper or printed out from a computer system. This may include working both on- site or remotely (e.g. at home)
- Stored in structured manual filing systems
- Transmitted by electronic mail, fax, over the Internet and via wireless technology
- Stored and processed via computers, computer networks or mobile computing de
- Devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs).
- Stored on **any** type of removable computer media including, but not restricted to CDs, DVDs, tapes, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

1.1 Purpose of Policy

The purpose of the Information Security Policy is:

- To protect the Parish Council's Information and subsequently to protect the Parish Council's reputation
- To enable secure information sharing to deliver services
- To protect the Parish Council from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect the Parish Council's employees

- NOT to constrain reasonable use of information in support of normal business activities of the Parish Council
- Ensure timely review of policy and procedure in response to feedback, legislation and other factors so as to improve ongoing security.

This policy shall be seen as additional to all other Parish Council policies relating to information disclosure and personal conduct.

1.2 Scope

This Information Systems Security Policy applies to all staff and members of the Parish Council, all third parties who interact with Council information, and all of the systems used to store or process it.

2. Policy

2.1 Breaches of the Information Security Policy

Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious.

Breaches of this policy by a user who is not a direct employee of the Parish Council may result in action being taken against the user and/or their employer.

In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated.

Breaches of the Data Protection Act 2018 could result in a hefty fine being issued to the individual and the organisation

2.2 Awareness and communication

All authorised users will be informed of the policy and of supporting policies and guidelines when their account is issued.

2.3 Definitions

Council Data includes all data elements that are owned or licenced by the Council or any information processed by the Council on behalf of a third party.

Council information systems - This includes but is not limited to all information systems owned, held, utilised or present on a Council network and anyone making use of them.

2.4 Information Security Principles

The following principles provide a framework for the security and management of the Council's information and information systems.

1. All individuals covered by the scope of this policy must handle information appropriately in accordance with its classification level.
2. Information should be only available to those with a legitimate need for access.

3. Information will be protected against unauthorised access and processing.
4. Information will be protected against loss and corruption.
5. Information will be disposed of securely and in a timely manner with measures appropriate for its classification.
6. Breaches of policy must be reported by anyone aware of the breach in a timely manner.

2.5. Legal and regulatory obligations

The Parish Council and its staff must adhere to all current UK and EU legislation as well as regulatory and contractual requirements.

2.6 Information Classification

The following table provides a summary of the Information Classification levels which are part of the Information Security Principles.

Category	Highly Restricted	Restricted	Internal Use
Description	• Highly confidential information whose inappropriate disclosure would be likely to cause serious damage or distress to individuals and/or constitute unfair/unlawful processing of "sensitive personal data" under the Data Protection Act; and/or • Seriously damage the Council's interests and reputation; and/or significantly threaten the security/safety of the Council and its staff.	• Confidential information whose inappropriate disclosure would be likely to cause a negative impact on individuals and/or constitute unfair/unlawful processing of "personal data" under the Data Protection Act; and/or damage the Council's interests, • and/or have some negative impact on the Council's reputation.	• Information not considered being • public which should be shared only • internally but would not cause • substantive damage to the Council • and/or individuals if disclose
Examples	• Sensitive personal data relating to identifiable living individuals • Individual's bank details • Non-public information that facilitates protection of individuals' safety or security of key	• Personal data relating to identifiable living individuals • Staff contact details	• Non-confidential internal correspondence e.g. routine administration such as meeting room and catering arrangements

	functions and assets e.g. network passwords and access codes for higher risk areas		• Final council meeting papers and minutes • Internal policies and procedures

3. Responsibilities

Individuals must adhere to the Acceptable Use Policy and follow relevant supporting procedures and guidance. An individual should only access systems and information they have a legitimate right to and not knowingly attempt to gain illegitimate access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data. In particular individuals should adhere to the information security 'dos and don'ts' outlined in the table below:

DO	**DO NOT**
Do use a strong password and change it if you think it may have been compromised	Don't give your password to anyone
Do report any loss or suspected loss of data	Don't reuse your Council password for any other account
Do be on your guard for fake emails or phone calls requesting confidential information - report anything suspicious to the clerk	Don't open suspicious documents or links
Do keep software up to date and use antivirus on all possible devices	Don't undermine the security of Council systems
Do be mindful of risks using public Wifi or computers	Don't provide access to Council information or systems
Do ensure Council data is stored on Council systems	Don't copy confidential Council information without permission
Do password protect and encrypt your personally owned devices	Don't leave your computers or phones unlocked

4. Reporting Information Security Breaches

It is vital that all users of information systems at the Parish Council comply with the information security policy. Any breach of information security is a serious matter and could lead to the possible loss of confidentiality, integrity or availability of personal or other confidential data. Such a loss may result in criminal or civil action against the Council and also the loss of reputation and financial penalties. Major breaches must be reported to the ICO within 72 hours

Any actual or suspected breach of this policy must be notified to the Chairman of the Council. All security incidents will be investigated and consequent actions may follow in line with this policy; Council disciplinary policy; and relevant laws.

Examples of incidents:

Breach of security

- Loss of computer equipment due to crime or an individual's carelessness

- Loss of computer media e.g. memory sticks
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident
- Finding the doors and/or windows have been broken and forced entry gained to a secure room/building that contains service user records

Breach of confidentiality/security

- Finding a computer print out with a header and a person's information on it at a location outside of Parish Council premises
- Finding any paper records about a service user/member of staff or business of the organisation in any location outside of the Parish Council premises
- Being able to view service user records in the back (or front) of an employees car
- Discussing service user or staff personal information with someone else in an open area where the conversation can be overheard
- A fax being received by the incorrect recipient

5. Passwords

1. Never reveal your password to anyone else or ask others for their password.

2. When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.

3. There is a useful tool that will help identify how strong a password you are using – check your password out at http://www.microsoft.com/protect/yourself/password/checker.mspx

4. Users with administrative level access should ensure that they utilise a complex password – 6 random character/numbers in mixed case.

5. If you forget your password, please request that it be reset

6. If you believe that other people may have discovered your password, then change it *immediately*

7. Never use the feature 'Remember password'

8. Change passwords regularly

9. Never leave your computer unattended while using any personal data – if called away you should lock the workstation – this will normally require a password to reopen

10. Never allow another person to login to any system with your login ID and password. Auditing measures in place could result in you being responsible for the actions of another person.

11. Never write your password down and leave it out for others to find.

6. USB Memory Stick Policy / Removable Hardware

Despite their small size, USB memory sticks have a very large capacity and therefore pose a considerable security risk if they are lost, stolen or abused.

The Parish Council does allow the use of memory sticks but only if they are encrypted and supplied by the Parish Council. All other memory sticks, especially unencrypted, are banned.

All removable hardware must be encrypted.

7. Working from home

All paper records which contain personal data need to be secure e.g. lock them away when not in use. Do not allow family or friends see any personal data. Family and friends should not use any council ICT equipment or email accounts.

8. Email Security

When sending an email which contain personal data, you must ensure that they are sent securely sending confidential information securely by e.g. encryption, password protection on attachments etc

When sending emails to multiple recipients, always use the BCC field. If you have received an email which has been sent to multiple recipients, do not 'Reply to All' if your response contains personal data, as the other recipients may not be authorised to see this data.

9. Policy review

The Council will review this policy when required to ensure that it remains appropriate and up to date.