Holford Parish Council

Information Technology Policy

Adopted: 8th September 2025

Introduction

Holford Parish Council recognises that information and the associated processes, systems and networks are valuable assets, and that the management of personal data has important implications for individuals.

The Council understands that the security of information is essential. The policy below is to protect all information assets owned and used by Holford Parish Council (HPC). This policy includes recommendations contained in ISO 27001 (previously British Standard 7799) – A Code of Practice for Information Security Management.

Definition

Information Security is defined as the preservation of:
- Confidentiality: protecting information from unauthorised access and disclosure.
- Integrity: safeguarding its accuracy and completeness; and
- Availability: ensuring that information is available to authorised users when required.

Information exists in many forms. It may be on paper, stored electronically, transmitted over a network, viewed in videos or films, or spoken in conversation. Whatever its form, or medium, appropriate protection is required to protect business continuity and to avoid breaches of the law, statutory, regulatory or contractual obligations.

All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Privacy

Privacy of Information It should be noted that HPC is a public body and will seek to carry out its business in a public and transparent way. Much of its business is conducted in meetings open to the public.

All information given at a public meeting of HPC is in the public domain, is likely to appear in the minutes and may be reported by the press.

The Council publishes many of its documents on its website. Although the Council owns some IT equipment, this is limited, and much business (principally by email) is conducted on Members' personal devices.

Protection of Personal Information.

The Council may hold and use information about employees, councillors, members of the public, and other data subjects for essential administrative and business purposes.

When handling such information, the Council, must comply with the Data Protection Principles which are set out in the General Data Protection Regulation (GDPR).

Responsibility for Information Security

Information security is the responsibility of all Members, employees (temporary or permanent), contractors, agents and anyone else processing information on our behalf.

Every person handling information or using Council equipment IT is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the Council.

Members should have no expectation of privacy in their use of any HPC business system. Any correspondence, documents, records or handwritten notes, may be disclosable to the public, under the Freedom of Information Act 2000 or the General Data Protection Regulation legislation. Any comments recorded or notes written must therefore be appropriate.

Compliance with Legal and Contractual Requirements

Use of HPC equipment

Where Council IT facilities are provided, they must only be used for authorised purposes. Limited personal use is permitted, provided that it doesn't interfere with council business.

Use of Personal equipment

Members and staff conducting Council business on their own personal equipment have a responsibility to follow established Good Practice to protect against malicious software and unauthorised external access to networks and systems.

Information should be regularly backed up.

HPC software should not be copied without authority, nor should copies of HPC information be made for personal use.

Access to HPC Information

Although the privacy of users' own files will be respected, the Council must reserve the right to examine systems, directories, files and their contents, on personal equipment e.g., laptops, iPads and mobile phones provided that there is a legitimate reason to do so (and you have told the member of staff that you can do this) such as a Freedom of Information request, subject access request or a request from the Information Commissioners Office (ICO). This is to confirm compliance with the legal and statutory regulations.

Authorisation for access must be obtained from the Clerk, or the Chair. Access shall be limited to the least action necessary to resolve the situation.

It should be noted that a GDPR issue could result in devices being held by the ICO during an investigation which can take up to a year.

Social Media and Online Participation

This policy includes Social Media and Online Participation, i.e., forums, blogs, websites and so on.
Members and staff should not disclose personal information about HPC's staff, members or business online, unless expressly authorised to do so. Members using social media should always be aware of their association with the Council and make sure that their posting is consistent with this.

Members are personally responsible and liable for the content they publish. They should be mindful that posts might remain public indefinitely.

Passwords

All mobile devices (phones, tablets, laptops) used for council business must be protected using passcodes, passwords, or biometric locks.
Passwords and passcodes must be strong and not easily guessed.
Removable media (such as USB drives) must be encrypted or password-protected when containing sensitive council data.

Retention and Disposal of Information

All members and staff have a responsibility to consider security when disposing of information in whatever medium and format it is kept. Specifically, all personal information shall only be retained for no longer than is necessary to complete the Councils business and should then be destroyed in line with the guidelines laid out in the Records Management Policy

Reporting

All staff and members should report immediately to the Clerk;
• any observed or suspected security incidents where a breach of the Council's security policies has occurred;
• any security weaknesses in, or threats to, systems or services; and
• any Software malfunctions