Salt and Enson Parish Council

IT & Digital Communications Policy

1. Introduction

Salt and Enson Parish Council recognises that information technology (IT) and digital communications are essential tools for the effective administration of the Council. This policy sets out how IT systems, digital devices, email, websites, social media and data are to be used, managed and protected.

This policy applies to all Councillors, the Clerk/RFO, employees, contractors and any other person authorised to use Council IT systems or access Council data.

2. Aims of the Policy

The aims of this policy are to: - Ensure IT systems are used lawfully, responsibly and effectively - Protect the confidentiality, integrity and availability of Council information - Reduce the risk of data loss, cybercrime and misuse of IT systems - Support compliance with relevant legislation and best practice

3. Scope

This policy covers: - Council-owned IT equipment (e.g. laptops, tablets, phones) - Personal devices used for Council business - Email systems and electronic communications - The Council website and social media accounts - Cloud storage and software systems - Data storage, backup and security

4. Legislative and Regulatory Framework

This policy should be read in conjunction with: - UK GDPR and the Data Protection Act 2018 - Freedom of Information Act 2000 - Local Government Transparency Code - Computer Misuse Act 1990 - The Council's Data Protection Policy - The Council's Social Media Policy

5. Responsibilities

5.1 The Council

The Council is responsible for: - Approving and reviewing this policy - Ensuring appropriate IT resources are available - Ensuring adequate security and backup arrangements are in place

5.2 Clerk / Responsible Financial Officer (RFO)

The Clerk/RFO is responsible for: - Day-to-day management of IT systems - Ensuring data is stored securely - Implementing security measures and updates - Reporting any data breaches or IT incidents

5.3 Councillors

Councillors are responsible for: - Using IT systems appropriately and securely - Protecting passwords and access credentials - Reporting any suspected security incidents immediately

6. Acceptable Use

Council IT systems must only be used for legitimate Council business. Users must not: - Access or distribute offensive, illegal or inappropriate material - Use Council systems for excessive personal use - Download unauthorised software - Circumvent security measures

Personal use of Council IT equipment should be minimal and must not interfere with Council business.

7. Email and Electronic Communications

- All official Council correspondence should be conducted via Council-provided email accounts where possible
- Emails relating to Council business are Council records and may be subject to FOI requests
- Care must be taken when sending personal or sensitive data by email
- Group emails should use BCC where appropriate to protect privacy

8. Passwords and Access Control

- Strong passwords must be used and kept confidential
- Passwords must not be shared
- Devices should be locked when not in use
- Access rights should be limited to what is necessary for the user's role

9. Data Storage and Backup

- Council data should be stored in approved locations only
- Regular backups must be maintained
- Data must not be stored permanently on unencrypted personal devices
- Confidential data must be encrypted where appropriate

10. Use of Personal Devices (BYOD)

Where personal devices are used for Council business: - Reasonable security measures must be in place (passwords, PINs, encryption) - Council data must be deleted when no longer required or when the individual leaves office - The Council reserves the right to request deletion of Council data from personal devices

11. Website Management

- The Council website will be maintained to provide accurate, up-to-date information

- Statutory information must be published in accordance with legal requirements
- Content must be approved in line with Council procedures

12. Social Media

- Social media accounts are official communication channels of the Council
- Only authorised persons may post on behalf of the Council
- Content must be factual, respectful and non-political
- Social media must not be used to disclose confidential or personal data

13. Cyber Security and Viruses

- Anti-virus and security software must be kept up to date
- Suspicious emails or attachments must not be opened
- Any suspected cyber incident must be reported immediately to the Clerk

14. Data Breaches and IT Incidents

- Any actual or suspected data breach must be reported immediately
- The Clerk will assess and, where required, report the breach to the Information Commissioner's Office (ICO)
- Incidents will be recorded and reviewed to prevent recurrence

15. Training

Appropriate IT and data protection training will be provided to Councillors and staff as required.

16. Monitoring

The Council reserves the right to monitor use of its IT systems where necessary and lawful, for: - Security purposes - Investigating suspected misuse - Compliance with legislation

17. Review of Policy

This policy will be reviewed at least every two years, or sooner if required by changes in legislation or technology.

Adopted by Salt and Enson Parish Council: 2nd September 2026

Review date: May 2027