DEEPING ST JAMES PARISH COUNCIL

The Institute, 38 Church Street, Deeping St James, Peterborough PE6 8HD
e-mail: clerk@deepingstjames-pc.gov.uk Tel: 01778 343266
Webpage: deeping-st-james.parish.lincolnshire.gov.uk
Parish Clerk: Julie Fortnum

Information Technology and Email Policy

1. Introduction

Deeping St James Parish Council recognises that effective, secure, and responsible use of Information Technology (IT) and email is vital to the council's operations, communications, and service delivery. This policy sets out the standards and procedures for all users to protect council information, ensure compliance with legal requirements, and maintain public trust.

2. Scope

This policy applies to:
- All councillors, employees, volunteers, and contractors who use council IT resources.
- All devices, networks, systems, software, and accounts used for council purposes, whether council-owned or personal devices (Bring Your Own Device – BYOD).
- All data, including email communications, files, cloud services, and records.

3. Legal and Regulatory Compliance

All IT and email usage must comply with:
- UK GDPR & Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
- Surveillance Camera Code of Practice (where CCTV is in use)

4. Acceptable Use

- Council IT resources must be used primarily for official council business.
- Limited personal use is permitted if it does not interfere with work duties or breach this policy.
- Users must avoid accessing, storing, or transmitting offensive, discriminatory, or unlawful material.
- Users must respect copyright and intellectual property rights.

5. Device and Software Management

- Only authorised devices and approved software may be used for council work.
- Installation of unapproved software or hardware on council devices is prohibited.
- All devices used for council work must have up-to-date security patches, antivirus

protection, and encryption enabled.
- BYOD use must comply with council security requirements (including password protection and encryption).

6. Data Security & Privacy

- Confidential and sensitive information must be stored securely and transmitted only via approved secure methods.
- Portable storage devices (e.g., USB sticks) must be encrypted.
- Cloud storage services must be approved by the council and comply with UK data protection laws.
- Data must be regularly backed up in line with council procedures.
- Disposal of old IT equipment must follow secure data destruction protocols.

7. Network & Internet Use

- The council's network and internet connections must be used responsibly and primarily for council purposes.
- Downloading or sharing copyrighted material without permission is prohibited.
- Public Wi-Fi connections must only be used with a secure VPN when accessing council data.

8. Email Use

- Official council email accounts must be used for council business.
- Emails should be professional, respectful, and relevant to council work.
- Sensitive information must be encrypted before sending.
- Be alert to phishing emails – verify links and attachments before opening.
- Auto-forwarding of council email to personal accounts is prohibited.

9. Password & Account Security

- Passwords must be strong (minimum 12 characters, with a mix of letters, numbers, and symbols) and unique for each system.
- Passwords must never be shared.
- Multi-Factor Authentication (MFA) must be used wherever available.
- Accounts will be deactivated when a user leaves the council.

10. Mobile Devices & Remote Working

- Mobile devices must be secured with a passcode or biometric lock.
- Lost or stolen devices must be reported immediately.
- Remote working must follow the same data security standards as office working.

11. Monitoring & Audit

- The council reserves the right to monitor IT and email use to ensure compliance with this policy and relevant legislation.
- Monitoring will be proportionate and in line with the Data Protection Act and UK GDPR.

12. Records Retention & Archiving

- Email and electronic records must be retained in accordance with the council's Records Management Policy.
- Unnecessary or duplicate records should be deleted regularly to reduce data storage risks.

13. Incident Reporting

- All suspected IT security incidents, breaches, or data loss must be reported immediately to the Parish Clerk (or designated IT contact).
- Cyber incidents may also be reported to the National Cyber Security Centre (NCSC) if required.

14. Training & Awareness

- All users will receive training on IT security, data protection, and safe use of council systems.
- Refresher training will be provided at least annually or when significant threats emerge.

15. Enforcement

Breaches of this policy may result in:

- Suspension or withdrawal of IT access.
- Disciplinary action in line with council procedures.
- Legal action if applicable.

16. Review

This policy will be reviewed annually, or sooner if legislation, technology, or operational needs change.