



CROOKHAM VILLAGE PARISH COUNCIL

Information Technology Policy

1. Purpose

This policy sets out the acceptable use of Crookham Village Parish Council's information technology systems, electronic communications, and digital services.

1.1 The purpose of this policy is to ensure that:

- 1.1.1 council information is protected from loss, unauthorised access, or misuse
- 1.1.2 council systems are used appropriately and lawfully
- 1.1.3 council business is conducted using secure and accountable communication channels
- 1.1.4 the council complies with its legal obligations under the UK GDPR, Data Protection Act 2018, Freedom of Information Act 2000 and other relevant legislation

1.2 This policy applies to councillors, employees, contractors, volunteers, and anyone using council systems or handling council information.

2. Scope

2.1 This policy applies to:

- 2.1.1 council computers, laptops, tablets and mobile devices
- 2.1.2 council email accounts
- 2.1.3 cloud storage and shared drives
- 2.1.4 council websites and online systems
- 2.1.5 council owned or council managed software and applications
- 2.1.6 personal devices used for council business (Bring Your Own Device – BYOD)

3. Acceptable use of Council IT

3.1 Council IT systems must be used responsibly and primarily for council business.

3.2 Users must:

- 3.2.1 use systems in a lawful and ethical manner
- 3.2.2 take reasonable steps to protect council information
- 3.2.3 comply with council policies relating to data protection and information governance
- 3.2.4 report any suspected security incidents immediately

4. Prohibited Use

4.1 Users must not:

- 4.1.1 access, store, transmit or publish illegal material
- 4.1.2 install unauthorised software on council systems
- 4.1.3 attempt to bypass security controls or access systems without authorisation
- 4.1.4 use council systems for harassment, discrimination, or offensive behaviour
- 4.1.5 knowingly introduce viruses, malware, or other harmful software
- 4.1.6 use council systems for personal commercial gain

5. Council Email Accounts and Domain Use

- 5.1 Council business should be conducted using council controlled email accounts wherever reasonably practicable.
- 5.2 Councillors and staff should use council email accounts for official communication relating to council business.
- 5.3 Personal email accounts should not normally be used for council business. Where this occurs in exceptional circumstances, the relevant emails must be copied or forwarded promptly to the appropriate council account or records system so that they form part of the council's official records.
- 5.4 Council email accounts remain the property of the council and may be accessed by authorised officers where necessary for lawful council purposes including business continuity, information requests, investigation of incidents, or security monitoring.

6. Non Corporate Communication Channels

- 6.1 Messaging services such as WhatsApp, SMS, Signal, Facebook Messenger, or similar platforms should not normally be used for substantive council business.
- 6.2 Where such channels are used in exceptional circumstances, users must ensure that any information relating to council business is transferred to the council's official systems as soon as reasonably practicable.
- 6.3 Users must cooperate with the council where official information relating to council business exists within private communication channels and may be required for:
 - 6.3.1 Freedom of Information requests
 - 6.3.2 Environmental Information Regulations requests
 - 6.3.3 Subject Access Requests
 - 6.3.4 complaints investigations
 - 6.3.5 audits or legal proceedings

7. Passwords and Authentication

- 7.1 Users must protect council systems and accounts through appropriate authentication controls.
- 7.2 Users must:
 - 7.2.1 use strong passwords for council systems

- 7.2.2 ensure passwords are not shared with others
- 7.2.3 avoid re-using passwords across multiple systems
- 7.2.4 enable multi-factor authentication where available

7.3 Passwords should be kept confidential and stored securely.

8. Device Security

8.1 All devices used to access council systems must have appropriate security controls.

8.2 Devices must:

- 8.2.1 be protected by a password or secure login
- 8.2.2 automatically lock after a period of inactivity
- 8.2.3 have up-to-date operating systems and security updates
- 8.2.4 use antivirus or anti-malware protection where applicable

8.3 Users must take reasonable precautions to prevent loss, theft, or unauthorised access to devices containing council information.

9. Bring Your Own Device (BYOD)

9.1 Personal devices may be used for council business where appropriate, provided reasonable security controls are in place.

9.2 Where personal devices are used for council work:

- 9.2.1 devices must be protected with passwords and screen lock
- 9.2.2 devices must have current operating system updates installed
- 9.2.3 council information should be stored within approved council systems where possible
- 9.2.4 users must report lost or stolen devices that contain council information immediately

9.3 Users must ensure council data is removed from personal devices when it is no longer required for council business.

10. Remote Working

10.1 Council systems may be accessed remotely where appropriate for council business.

10.2 Users accessing council systems from home or other remote locations must ensure that:

- 10.2.1 council devices and personal devices used for council work are protected with passwords and secure login
- 10.2.2 devices are not left unattended while logged into council systems
- 10.2.3 council information is not visible to unauthorised individuals
- 10.2.4 secure internet connections are used wherever possible
- 10.2.5 council data is not stored locally on personal devices unless necessary

10.2.6 paper records containing personal or confidential information must be handled securely and not left accessible to unauthorised individuals

10.3 Users must take reasonable precautions to protect council information when working outside council premises.

11. Storage of Council Information

11.1 Council information should be stored within approved council systems such as secure cloud storage, shared drives, or authorised applications.

11.2 Users should avoid storing council information solely on local devices or personal accounts.

11.3 Access to council systems and information must be restricted to authorised users who require access for their role.

12. Email Management and Retention

12.1 Council email accounts are a communication tool and should not be relied upon as the long-term storage location for council records.

12.2 Emails that form part of the council's official records should be saved to the appropriate council files or systems.

12.3 Email retention and deletion must follow the council's Retention and Disposal Policy.

12.4 Routine or transitory emails that do not form part of the council's records may be deleted when no longer required.

12.5 Emails must not be deleted where they may be required for:

12.5.1 Freedom of Information requests

12.5.2 Subject Access Requests

12.5.3 complaints investigations

12.5.4 insurance claims

12.5.5 legal proceedings

12.5.6 audit purposes

13. Data Security and Encryption

13.1 Sensitive or personal information should only be transmitted electronically where necessary and appropriate.

13.2 Where personal or confidential information is transmitted electronically, users should use appropriate safeguards such as:

13.2.1 secure cloud sharing

13.2.2 password-protected documents

13.2.3 encrypted attachments

13.3 Passwords protecting documents should be communicated separately where possible.

14. Incident Reporting and Data Breaches

- 14.1 Any suspected IT security incident or personal data breach must be reported immediately to the Clerk.
- 14.2 The Council's IT support provider may be contacted where technical assistance is required.
- 14.3 Examples include:
 - 14.3.1 sending information to the wrong recipient
 - 14.3.2 loss or theft of a device containing council data
 - 14.3.3 unauthorised access to council systems
 - 14.3.4 malware or phishing attacks
- 14.4 The Clerk will assess the incident and take appropriate action, including reporting to the Information Commissioner's Office where required under the council's Data Breach Policy.
- 14.5 All breaches and security incidents will be recorded and investigated.

15. Phishing and Cyber Security

- 15.1 Users should remain alert to phishing emails, suspicious attachments, or unusual system behaviour.
- 15.2 Users must not open suspicious attachments or click unknown links.
- 15.3 Any suspected phishing attempts should be reported immediately.

16. Monitoring and System Administration

- 16.1 The council may monitor the use of its systems where necessary for legitimate purposes including:
 - 16.1.1 maintaining system security
 - 16.1.2 protecting council data
 - 16.1.3 investigating suspected misuse
 - 16.1.4 ensuring business continuity
- 16.2 Any monitoring will be carried out lawfully and proportionately.

17. IT Assets and System Access

- 17.1 The council will maintain appropriate oversight of its IT assets, systems, and accounts.
- 17.2 Access to systems and shared resources should be limited to those who require access for their role.
- 17.3 Access permissions should be reviewed periodically and removed where no longer required.
- 17.4 When a councillor, employee, or contractor ceases their role, appropriate steps must be taken to ensure that access to council systems is removed and that all council information remains accessible to the Council.
- 17.5 Any councillor, employee, contractor or volunteer who ceases their role and who has accessed or stored Council information on personal devices, personal email accounts or personal storage systems must securely delete such

information when no longer lawfully required and, where requested by the Council, sign a declaration confirming that this has been completed.

18. IT Governance and Oversight

- 18.1 The Council will maintain appropriate oversight of its information technology systems and digital services to ensure security, continuity and compliance.
- 18.2 The Council will maintain a record of its key IT systems, software platforms and service providers used to process or store council information.
- 18.3 Responsibility for administration of council IT systems will be clearly assigned to appropriate officers or authorised service providers.
- 18.4 The Council will maintain an inventory of council owned IT equipment and devices used for council business.
- 18.5 Access to council systems will be granted only where necessary for official duties and will be removed when access is no longer required.
- 18.6 Where external IT service providers support council systems, appropriate contractual arrangements and security expectations will be in place.
- 18.7 Regular updates and security patches (software updates that fix security vulnerabilities) should be applied to council systems and devices wherever possible.
- 18.8 The Council will review its IT arrangements and security controls at least annually to ensure they remain appropriate for the Council's operational needs.

19. Compliance

- 19.1 All users must comply with this policy.
- 19.2 Failure to follow the policy may result in disciplinary action for staff or appropriate action under council governance arrangements for councillors.

20. Review

This policy will be reviewed periodically and updated where necessary to reflect changes in legislation, technology, or council operations.