



Noak Bridge Parish Council

Information Technology Policy

Version	Date Adopted	Minute Reference	Review Date
1	23 rd July 2025	78/2025/01	July 2026
2	24 th June 2026	77/2026/01	June 2027

Information Technology Policy

1. Introduction

1.1 Noak Bridge Parish Council recognises the importance of effective, secure and responsible use of information technology in supporting the Council's business, operations and communications.

1.2 This policy establishes the standards and responsibilities for the use of Council information technology systems, equipment, email accounts and data by councillors, employees, volunteers and authorised representatives.

1.3 This policy should be read in conjunction with the Council's Data Protection Policy, Social Media Policy, Code of Conduct, Standing Orders and any other relevant Council policies.

2. Scope

2.1 This policy applies to all councillors, employees, volunteers and authorised representatives who access or use Council information, systems, email accounts or technology, whether using Council-owned or personal devices.

3. Acceptable Use of IT Resources

3.1 Council IT resources must be used primarily for official Council business and activities.

3.2 Limited personal use is permitted provided that it:

3.2.1 Does not interfere with Council duties.

3.2.2 Does not incur additional costs to the Council.

3.2.3 Does not compromise security.

3.2.4 Does not breach any Council policy or legal requirement.

3.3 Users must act responsibly and professionally when using Council IT resources and must not:

3.3.1 Access, create, store or distribute offensive, discriminatory, defamatory or unlawful material.

3.3.2 Download or distribute copyrighted material without permission.

3.3.3 Use Council systems for political campaigning or party-political purposes.

3.3.4 Deliberately introduce malware, viruses or other harmful software.

4. Council Email Accounts

4.1 All councillors and the Clerk shall be provided with a dedicated Council email address ending "@noakbridgeparishcouncil.gov.uk".

4.2 The Council email address shall be used for all Council business, correspondence, communications, records and interactions relating to Council functions.

4.3 Personal email accounts must not be used for Council business except in exceptional circumstances where access to the Council account is temporarily unavailable.

4.4 Where Council business is conducted through a personal email account in exceptional circumstances, the communication must be forwarded to the individual's Council email account as soon as reasonably practicable to ensure proper record keeping and compliance with the Freedom of Information Act 2000 and Data Protection legislation.

4.5 Council email accounts remain the property of Noak Bridge Parish Council.

4.6 Users must not share passwords or allow unauthorised access to Council email accounts.

4.7 Emails sent from Council accounts must be professional, respectful and appropriate at all times.

5. Device and Software Usage

5.1 The Council currently provides one Council-owned laptop for use by the Clerk.

5.2 Councillors are permitted to access Council email accounts and Council information using their own devices.

5.3 Any device used to access Council systems or Council information must:

5.3.1 Be protected by a password, PIN or biometric authentication.

5.3.2 Be kept updated with current operating system and security updates.

5.3.3 Have appropriate anti-virus or security software installed where applicable.

5.3.4 Be used in a manner that protects Council information from unauthorised access.

5.4 Unauthorised software must not be installed on Council-owned equipment.

5.5 Personal USB storage devices should not be used on Council-owned equipment unless necessary and approved by the Clerk.

6. Data Management and Security

6.1 All Council information must be stored, transmitted and managed securely.

6.2 Personal data must be processed in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Council's Data Protection Policy.

6.3 Confidential or sensitive information must only be shared with authorised persons.

6.4 Council information should not be stored on personal cloud storage services unless specifically authorised by the Council.

6.5 Council records must be retained and disposed of in accordance with legal requirements and the Council's retention arrangements.

7. Passwords and Account Security

7.1 Users are responsible for maintaining the security of their accounts and passwords.

7.2 Passwords should follow current best practice and consist of strong, unique passwords, preferably using three random words.

7.3 Passwords must not be shared with any other person.

7.4 Multi-Factor Authentication (MFA) must be enabled wherever available on:

7.4.1 Council email accounts.

7.4.2 Website administration accounts.

7.4.3 Cloud storage systems.

7.4.4 Any other Council systems containing sensitive information.

7.5 Passwords should be changed immediately if there is any suspicion that they have been compromised.

8. Network and Internet Usage

8.1 Internet access should be used responsibly and primarily for Council business.

8.2 Users must not knowingly visit malicious, unlawful or inappropriate websites using Council systems.

8.3 Downloading, distributing or sharing copyrighted material without authorisation is prohibited.

9. Remote Working and Mobile Devices

9.1 Users accessing Council information away from their normal place of work must take reasonable precautions to protect information and equipment.

9.2 Particular care must be taken when:

9.2.1 Using public Wi-Fi networks.

9.2.2 Working in public places.

9.2.3 Viewing confidential information where it may be seen by others.

9.3 Devices used to access Council information must not be left unattended in public places or unsecured vehicles.

9.4 Printed documents containing Council information must be securely stored and disposed of appropriately.

10. Social Media

10.1 The use of social media is governed by the Council's Social Media Policy.

10.2 Councillors, employees and authorised representatives must comply with the Social Media Policy when using official Council accounts or discussing Council business online.

11. Monitoring

11.1 The Council reserves the right to monitor and review the use of Council IT systems and email accounts where there is a legitimate business, security or legal reason for doing so.

11.2 Any monitoring will be conducted in accordance with applicable legislation, including the UK GDPR and Data Protection Act 2018.

12. Reporting Security Incidents

12.1 All suspected or actual security incidents must be reported to the Clerk immediately.

12.2 Security incidents include, but are not limited to:

12.2.1 Loss or theft of a device containing Council information.

12.2.2 Suspected phishing emails.

12.2.3 Malware infections.

12.2.4 Unauthorised access to accounts.

12.2.5 Disclosure of confidential information.

12.2.6 Personal data breaches.

12.3 The Clerk shall ensure that appropriate action is taken and, where necessary, that any data breach is assessed and reported in accordance with legal requirements.

13. Training and Awareness

13.1 The Council will promote awareness of cyber security, data protection and information governance responsibilities.

13.2 Councillors and employees are expected to undertake any relevant training provided or recommended by the Council.

14. Compliance and Consequences

14.1 Failure to comply with this policy may result in the withdrawal of access to Council systems and may lead to disciplinary or other appropriate action.

14.2 Serious breaches may constitute misconduct, breaches of the Councillors' Code of Conduct, or breaches of statutory obligations.

15. Policy Review

15.1 This policy will be reviewed annually or sooner if required by changes in legislation, guidance or Council operations.

16. Contact

16.1 For IT-related enquiries, support or to report a security incident, contact:

16.1.1 The Parish Clerk.

16.1.2 clerk@noakbridgeparishcouncil.gov.uk

16.2 By adhering to this policy, councillors, employees and authorised representatives contribute to maintaining a secure, efficient and compliant information technology environment for Noak Bridge Parish Council.