KIRK ELLA & WEST ELLA PARISH COUNCIL
INFORMATION TECHNOLOGY POLICY

INTRODUCTION

This IT policy has been tailored to reflect the specific circumstances of Kirk Ella & West Ella Parish Council. The Council has one employee (the Clerk) who works remotely, and councillors are unpaid volunteers who use their own personal devices for council business. The Council does not have physical premises.

PURPOSE OF THE IT POLICY

The purpose of this IT policy is to establish clear parameters for appropriate use of technology in the course of council duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Limited personal use of council-provided IT equipment (applicable to the Clerk only) is permitted, provided it does not interfere with council work and is restricted to breaks or non-working hours.

MONITORING OF ITS USE

As an IT provider, the Council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and the Clerk is informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. This applies to council email addresses and systems accessed by both the Clerk and Councillors.

SCOPE OF THIS POLICY

This policy applies to:

- The Clerk (the Council's sole employee), who is provided with council IT equipment and works remotely;
- All Councillors, who are unpaid volunteers and use their own personal devices for council business.

COMPUTER USE

Hardware

1. Council computer equipment provided to the Clerk is for council purposes, however reasonable personal use is permitted (as determined by the Council). Any personal use should not interrupt council work and should be restricted to breaks or outside working hours.

2. The Clerk must lock their computer when stepping away to prevent unauthorised access. This applies to all council-provided devices. Councillors should apply similar security practices to their personal devices when handling council business.

3. All computer and electronic equipment supplied to the Clerk should be treated with care at all times. Computer equipment is expensive, and any damage will have a financial impact on the Council.

4. Computer and electronic hardware should be kept clean, with precautions taken to prevent food and drink being spilled onto it.

5. All council-owned computer and mobile equipment will be logged and tracked. A register of equipment issued to the Clerk will be maintained.

6. Equipment should not be dismantled or reassembled without seeking advice from the Council.

7. The Clerk is not to purchase any computer or mobile equipment (including software) without prior authorisation from the Council.

8. Personal disks, USB sticks, CDs, DVDs, or other data storage devices cannot be used on council computers without the prior approval of the Council.

9. Any faults or necessary repairs must be reported to the Council.

EQUIPMENT

Portable Equipment (Clerk)

10. Portable equipment (laptop computer) is provided to the Clerk.

11. The Clerk must follow council backup procedures for portable equipment at all times, ensuring regular backups of council data.

12. All portable computers must be stored safely and securely when not in use. Equipment should not be left unattended in public places and should never be left in parked vehicles.

13. All portable devices must be protected with encryption in case they are lost or stolen. All smartphones or tablets with council email access must have PIN/password/biometric protection enabled.

14. Council-owned portable equipment should only be used on secure, password-protected networks. Public Wi-Fi should be avoided for sensitive council business unless using a VPN.

15. Loss or theft of any council equipment must be reported to the Council immediately, and to the Police if appropriate.

Personal Devices Used by Councillors (BYOD)

16. Councillors are unpaid volunteers who use their own personal devices to conduct council business. The Council does not provide IT equipment to Councillors.

17. When using personal devices for council business, Councillors should:

- Ensure devices have up-to-date anti-virus and security software;
- Use strong passwords and enable device encryption where possible;
- Not store sensitive council data on personal devices unless necessary, and delete it when no longer needed;
- Be cautious about using public Wi-Fi for council business;
- Report any loss or security concerns related to council data immediately.

18. Councillors should be aware that using personal devices for council business may mean those devices could be subject to Freedom of Information requests or legal proceedings relating to council matters.

Software

19. Only licensed or approved software may be installed on council-provided equipment. The Clerk must not install unauthorised software without approval from the Council.

20. Software licences and proof of purchase must be retained and made available for audit purposes.

21. All council-provided devices must have up-to-date anti-virus software installed and regularly updated.

PASSWORD AND AUTHENTICATION POLICY

22. All users (Clerk and Councillors) must use strong, unique passwords for council systems and email accounts. Passwords should be:

- At least 12 characters long;
- A mix of uppercase, lowercase, numbers, and special characters;
- Changed if there is any suspicion of compromise;
- Not shared with anyone or written down in accessible locations.

23. Multi-factor authentication (MFA) should be enabled on all council systems where available.

24. Default passwords on any new equipment or systems must be changed immediately upon receipt.

DATA PROTECTION AND BACKUPS

25. The Clerk is responsible for ensuring regular backups of all council data. Backups should be encrypted and stored securely, preferably using cloud-based services with appropriate security measures.

26. All council data must be handled in accordance with the Data Protection Act 2018 and UK GDPR. Personal data should only be collected, stored, and processed for legitimate council purposes.

27. Council data should not be stored on personal devices unless absolutely necessary, and should be deleted securely when no longer needed.

REMOTE WORKING

The Council does not have physical premises, so the Clerk works remotely by default. This section sets out expectations for remote working practices.

28. The Clerk must ensure their remote working environment is secure and private when handling confidential council matters.

29. Video conferencing and online meetings should be conducted using secure platforms with appropriate access controls (passwords, waiting rooms).

30. Council equipment should be kept secure at the Clerk's home and not accessed by unauthorised persons.

31. The Council should ensure adequate insurance coverage for council equipment kept at their home.

EMAIL

32. Council email accounts must only be used for legitimate council business. Limited personal use by the Clerk is permitted as outlined earlier in this policy.

33. Users must be vigilant about phishing attempts and suspicious emails. Do not click links or download attachments from unknown or suspicious sources.

34. Email signatures should include appropriate council contact information and, where relevant, disclaimers.

35. Confidential or sensitive information should not be sent via email unless encrypted or using secure file transfer methods.

36. All email communications must be professional, courteous, and comply with the Council's code of conduct.

37. Auto-forwarding of council emails to personal email accounts is not permitted without authorisation from the Council.

USE OF THE INTERNET

38. The following activities are prohibited when using council equipment or conducting council business:

- Accessing, downloading, or distributing illegal, offensive, or inappropriate material;
- Downloading or installing unauthorised software;
- Engaging in gambling, gaming, or other non-work-related activities during working hours;
- Using council resources for personal financial gain;
- Any activity that could damage the Council's reputation or breach its Code of Conduct.

39. Users should be aware that internet activity may be monitored where there is a legitimate reason to do so.

USE OF SOCIAL MEDIA

This section applies to both the Clerk and Councillors when using social media in relation to their council role or when posting content that could affect the Council.

- Council database contacts should not be connected with on LinkedIn or other social networking sites unless authorised.
- Any blog or social media post mentioning the Council should identify the author and clearly state that views expressed are their own and do not represent the Council's views. Use a disclaimer such as: "The comments and other content are my own and do not represent the positions or opinions of Kirk Ella & West Ella Parish Council."
- Councillors and the Clerk must be respectful about the Council and not engage in behaviour that will reflect negatively on its reputation. Unauthorised use of copyright materials, defamatory statements, or misrepresentation could constitute misconduct.
- Photos or videos that could reflect negatively on the Council should not be posted on social media. Photos, videos, or audio recordings must not be taken during council meetings without permission.
- Comments posted should be knowledgeable, accurate, professional, and should not compromise the Council in any way.
- Confidential or private council information must not be posted on social media. This includes non-public financial or operational information, personal information about others, or anything subject to confidentiality requirements. This does not affect statutory requirements to publish information under the Freedom of Information Act.
- Councillors should be mindful of the Members Code of Conduct and Nolan Principles when posting on social media. All users are personally liable for anything they post online.
- Media contacts relating to the Council should be referred to the Clerk or Chair as appropriate.
- If using social media for council development purposes, login details must be provided to the Council so accounts can be accessed in the user's absence.
- Upon leaving the Council, the Clerk must delete all council-related data from personal devices. Councillors should ensure their social media profiles are updated to reflect they are no longer Councillors.

MISUSE

Misuse of IT systems and equipment is not in line with the Council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to:

- For the Clerk: formal action, including disciplinary proceedings or dismissal;
- For Councillors: action under the Members Code of Conduct, potentially including referral to the Monitoring Officer.

POLICY REVIEW

This policy will be reviewed annually or when there are significant changes to the Council's IT arrangements, relevant legislation, or best practice guidance.