

KETTLEBURGH PARISH COUNCIL

IT & SOCIAL MEDIA POLICY

Title	Kettleburgh Parish Council IT & Social Media Policy
Drafted on	18 July 2026
Drafted by	Richard Green, Clerk and Interim RFO Cllr Louise Clark (social media provisions)
Adopted on	[DATE]
Minute reference	[MINUTE REF.]
Next review	By July 2027

1. Introduction

Kettleburgh Parish Council, hereinafter “KPC” recognises the importance of effective and secure use of information technology (IT), email, and social media in supporting its operations and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources, email, and social media by councillors, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, email accounts, and social media. KPC acknowledges that, as a small local authority, employees and councillors are likely to be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

3. Training and awareness

KPC will seek to provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. Regular training should be sought on email security and best practices, including but not limited to:

- the Parish Council Domain Helper Service’s virtual cybersecurity workshops for councils
- The National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

4. KPC-provided IT resources and email

When using IT resources for KPC purposes, you must adhere to ethical standards, respect copyright and intellectual property rights, and not use KPC-provided equipment or email accounts to access or forward inappropriate or offensive content.

Where possible, KPC will endeavour to provide or recommend relevant software and applications for work-related tasks. Check with the Clerk before using any software or application that has not previously been recommended so that they can ensure compliance with this and other relevant policies, and you must not use.

5. Use of personal devices

Where possible, KPC will endeavour to provide individuals with devices to use for council business. If using your own personal devices, please endeavour to always:

- use strong passwords for all your accounts (preferably using a password manager)
- download the latest operating system security updates
- use anti-virus software

6. Network and internet usage

Be careful about which Wi-Fi networks you join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted and password-protected internet connection when carrying out KPC-related activities.

7. Password and account security

You are responsible for maintaining the security of your accounts and passwords. Use the National Cyber Security Centre's [advice for choosing a strong password](#). For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

8. Email communication

KPC provides all employees and councillors with a .gov.uk email account for KPC-related communication only. Emails must be professional and respectful in tone. When sending any confidential or sensitive information, double-check that such information is being sent to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by carefully looking at the origin email address. Do not download or open anything if you are unsure who has sent it.

9. Email access

KPC reserves the right to check email communications to ensure compliance with this policy and relevant laws. Any monitoring will be conducted in full accordance with the Data Protection Act and GDPR. The Clerk may need to access emails in order to respond to FOI or subject-access requests.

10. Social media

a) Policy

KPC recognises that social media and networking websites are a regular part of day-to-day life. Many people engage with local/community groups and organisations through membership of digital networks such as Facebook and Instagram. Provisions a) to j) set out KPC's approach to the use of social media and digital networks. It defines the roles and

responsibilities within KPC for this area, and provides councillors and employees with guidelines on their responsibilities for the use of social media.

b) Purpose

KPC's aims include informing members of the community and the wider local area, through a variety of communication channels, about what is happening within the parish and local area and sharing important news and information. KPC's social media accounts and activity supplements the information published on its website and any newsletters it produces, e.g. PEDL.

KPC can:

- inform people of important events and alert followers in a timely way;
- provide links to useful and interesting information about the parish and local area published by other parties; and
- better communicate with those using mobile devices and personal computers.

c) Official social media accounts

KPC operates Facebook and Instagram accounts for the promotion of activities and events and as a communication and broadcast tool. Examples of acceptable content are:

- i. Consultation documents
- ii. News feed & emergency information
- iii. Key dates
- iv. Short comments on hot topics and relevant news
- v. Polls and information gathering
- vi. Useful links

d) Roles and responsibilities:

An official KPC account on any social media site may only be set up with approval of the full council. Access to and use of any account is restricted and managed by authorised roles in the following way:

Authorised roles:

The Clerk to KPC will be the official account holder and administrator. Up to two councillors will be nominated to manage content and support the administrator of any official account. The identified employees and nominated councillors will also manage any interface between KPC's social media accounts and its website. They will be responsible for liaising with KPC's website provider.

Only these authorised employees and councillors may use the social media account(s) to post information online and access to the account is strictly limited.

KPC's social media account(s) will be frequently managed and monitored by the Clerk with the support of the nominated councillors. The Clerk and/or nominated councillors may post links to KPC's website, partner websites, 'useful' links such as local transport sites, links to other Facebook pages, and local media including national organisations.

All information published on the internet must comply with the KPC's data protection policies. The social media account will primarily be used to promote 'good news' and information, supplementing content already published on KPC's website.

Any employee, councillor, or member of the public who becomes aware of social media activity that would be deemed distasteful should make the Clerk and/or nominated councillors aware as soon as possible.

e) Facebook and Instagram

The account holder/administrator manages KPC's Facebook and Instagram pages. These pages are used to highlight news, make announcements, engage with the community, and

share information. The accounts will not be set up to enable “comments” to be posted on KPC’s Facebook page. Requests for something to be posted on KPC’s Facebook page, should be directed to the account holder and/or nominated councillors.

f) Use of photos and video

Only the Clerk and/or nominated councillors have permission to upload photos and videos. The appropriate permissions must be obtained for all imagery.

g) Personal accounts on social media

Councillors and employees are likely to have personal social media accounts. Personal accounts need to be used in a way that does not conflict with the KPC’s Code of Conduct or terms of their contract of employment. The absence or lack of explicit reference to a specific website or service does not limit the extent of the application of this policy. Where no policy or guidelines exist, councillors or employees should use their professional judgment and take the most prudent action possible. If KPC is referred to in a way that is deemed defamatory or confidential information is disclosed, it reserves the right to report the comment and request that it be removed.

Councillors are at liberty to set up personal accounts using any of the tools available but should ensure they are clearly identified as personal and do not in any way imply that they reflect KPC’s view. Councillors should always present a professional image and not disclose anything of a confidential nature.

Comments of a derogatory, proprietary, or libellous nature should not be made and care should be taken to avoid guesswork, exaggeration, and colourful language.

h) Pre-election period of sensitivity

In the six-week run up to an election – local or general – councils have to be very careful not to do or say anything that could be viewed in any way to support any political party or candidate. The period is known as the pre-election period of sensitivity. KPC will continue to publish important service announcements using social media but will monitor and potentially must remove responses if they are overtly party political.

i) Direct messages on social media

If appropriate, the Clerk will endeavour to respond as quickly as possible to all questions received via the social media accounts.

All formal requests, comments, enquiries, or complaints should be emailed to the Clerk.

j) Rules

KPC may monitor forums and blogs to gain indirect feedback. KPC may post replies on forums or blogs to answer queries or address factual corrections but would generally take a cautious approach before getting involved in contentious issues.

KPC reserves the right to take any necessary steps to protect members of the parish community and will delete any comments referencing KPC which are deemed to be abusive or offensive in anyway.

11. Data management, data retention, and security

All sensitive and confidential data must be stored and transmitted securely. Any important data must be regularly backed up in order to prevent data loss and in accordance with KPC’s data retention policies.

Emails should be retained and archived in compliance with KPC’s data retention policies. Any unnecessary emails should be reviewed and deleted in order to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches, including email breaches or incidents should be reported immediately to the Clerk in their role as Data Protection Officer.

13. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

14. Contacts

For IT-related enquiries or assistance, users can contact the Clerk.