LOGGERHEADS PARISH COUNCIL
INTERNET, EMAIL AND SOCIAL MEDIA POLICY

Approved by Council: November 2023
Date of Review: May 2026

Introduction

Communications via email internet usage undertaken in the name of the Council or on Council systems carry inherent risks such as: -

- Potential defamation.
- Spreading of viruses, including Trojans which can steal date.
- Breach of confidentiality.
- Accepting files from sources in online chat rooms which could bypass firewalls or email filters.
- Breach of contract.
- Breach of copyright.
- Breach of data protection legislation.
- Breach of privacy and unlawful discrimination.

This policy sets out the restrictive use of the Parish Council's electronic equipment, namely, computers and telephones.

The Parish Council reserves the right to monitor telephone, email and internet usage in accordance with the law, in particular the latest Data Protection Act and the Human Rights Act. The Council provides telephones, email and internet access solely for the purposes required for the performance and fulfilment of job responsibilities.

Occasional and reasonable personal use of the Council's telephone, internet and email service is permitted, provided it does not interfere with work performance or security.

Monitoring and Privacy Issues

Internet and email usage may be monitored from time to time to identify potential breaches of this Policy. This may lead to formal disciplinary action. Employees should note that serious breaches may result in dismissal for gross misconduct.

However, the Parish Council is subject to Article 8 of the Human Rights Act, and this means that the Council will respect employees' private and family life.

Email Etiquette

All employees must follow the procedure outlined below when sending and receiving emails on behalf of the Parish Council: -

- Only agreed email signatures may be used.
- All messages must use appropriate business language.

- A waiver clause will be included at the end of each email message.
- The circulating of offensive, indecent or obscene material or anything which breaches the Equal Opportunities Policy is strictly prohibited.
- Confidential material should not be disclosed.
- Only attachments from a trusted source may be downloaded.
- Ensure that the address of the recipient is correct before sending emails.
- Ensure that a 'reply to all' is appropriate.
- Ensure that essential files are saved before deleting the message in which they were received.

Telephone Etiquette

All employees must follow the procedure outlined below when using the Council's telephone: -

- Answer all calls by stating the name of the Parish Council.
- Be always polite.
- Do not be rude or abrupt to callers.
- Do not use offensive language.
- Do not swear.
- Check the telephone frequently for messages from callers and respond in a timely manner.

Employees may make and receive personal calls if they are brief and infrequent. This applies to calls on the Council's land line or employees' personal mobile phones.

Unacceptable Behaviour on the Internet

Below are examples of what the Prish Council deems to be unacceptable use or behaviour by employees: -

- Allowing non-authorised users to access the internet using employees log in or while logged on.
- Visiting internet sites that contain obscene, hateful, pornographic or other illegal material.
- Passing on such material to colleagues or external people.
- Using the computer to perpetrate any form of fraud or software, film or music piracy.
- Using the internet to send offensive or harassing material to other users.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about the Council, its employees, members, colleagues and/or customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network.
- Gambling online.
- Disclosure of any confidential corporate information without express consent.
- Any other area that the Council reasonably believes may cause problems

Social Media

This section of the policy is intended to help Officers and Councillors make appropriate

decisions about the use of social media such as social networking websites, forums, message boards, blogs or comments on web-articles, such as Twitter, Facebook and LinkedIn.

This policy outlines the standards the Council requires employees and elected members to observe when using social media, the circumstances in which your use of social media will be monitored and the action that will be taken in respect of breaches of this policy.

All Officers and Councillors are expected to always comply with this policy to protect the privacy, confidentiality, and interests of the Council.

Breach of this policy by employees may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Breach of this policy by elected members will be dealt with under the Code of Conduct.

The Council has overall responsibility for the effective operation of this policy.

The Clerk is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our work.

All Officers and Councillors should ensure that they take the time to read and understand this policy. Any breach of this policy should be reported to the Clerk or Chair of the Council.

Questions regarding the content or application of this policy should be directed to the Clerk.

The Clerk and administration officer are permitted to post material on a social media website in the name of the Council and on its behalf in accordance with the rules and scope of this policy.

If you are not sure if your comments are appropriate do not post them until you have checked with the Clerk.

The Council recognises the importance of the internet in shaping public thinking about the Council and the support and services it provides to the community. It also recognises the importance of our employees and elected members joining in and helping shape community conversation and direction through interaction in social media.

Before using social media on any matter which might affect the interests of the Council you must have read and understood this policy, and Officers must have gained prior written approval to do so from the Clerk.

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules: -

- Do not upload, post or forward a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Any employee/elected member who feel that they have been harassed or bullied or are offended by material posted or uploaded by a colleague onto a social media website should inform the Clerk.
- Never disclose commercially sensitive, personal private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with the Clerk or Mayor.
- Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.
- Before you include a link to a third-party website, check that any terms and conditions

of that website permit you to link to it.

- When making use of any social media platform, you must read and comply with its terms of use.
- Be honest and open but be mindful of the impact your contribution might make to people's perceptions of the Council.
- You are personally responsible for content you publish into social media tools.
- Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations.
- Don't discuss colleagues without their prior approval.
- Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion. Remember that although it is acceptable to make political points or canvass votes via your own social media accounts this will not be permissible if you are commenting on behalf of the Council.
- Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details.

Employees and elected members should be aware that any use of social media websites (whether accessed for Council purposes) may be monitored and, where breaches of this policy are found, action may be taken against employees under our Disciplinary Procedure and councillors under the Code of Conduct.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the Council.

In particular a serious case of uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will probably amount to gross misconduct/breach of the Code of Conduct (this list is not exhaustive):-

a. pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).
b. a false and defamatory statement about any person or organisation.
c. material which is offensive, obscene, criminal, discriminatory, derogatory or may cause embarrassment to the Council our councillors or our employees.
d. confidential information about the council or anyone else.
e. any other statement which is likely to create any liability (whether criminal or civil, whether for you or the organisation).
f. material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action will be addressed under the Disciplinary Procedure/Code of Conduct.

Where evidence of misuse is found the Council may undertake a more detailed investigation involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.

If you notice any use of social media by other employees/elected members in breach of this policy, please report it to the Clerk in accordance with the Council's Whistleblowing Policy.

Monitoring and Review

The Council shall be responsible for reviewing this policy annually to ensure that it meets legal

requirements and reflects best practice.