



Internet, Email and Social Media Policy

Overview

Communications via email or 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, Malware or Ransomware which can steal data or encrypt data.
- Breach of confidentiality.
- Accepting the download of files or clicking on links from a variety of sources online or in emails which could bypass security 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 framework for use of the Town Council's electronic equipment, namely; computers and telephones, by Council employees and members.

The Town 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 that it does not interfere with work performance or security of the Council's IT Network.

Monitoring and Privacy Issues

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

However, the Town 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 Town Council:

- Only agreed email signatures may be used.
- All messages must use appropriate business language.
- A confidentiality and liability waiver clause will be included at the end of each email message, ideally as an email 'signature'.

- 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 to third parties.
- Only attachments and links from a trusted source(s) should be downloaded or clicked upon. Please be aware that even 'trusted' contacts can be compromised so careful analysis of the email received is pertinent before undertaking these actions.
- Ensure that the address of the recipient is correct before sending emails.
- Ensure that the use of 'reply to all' is appropriate.
- Ensure that essential files are saved before deleting the message in which they were received.
- In the event of any amount of uncertainty please contact the Council's IT Consultant in the first instance.

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 Town Council.
- Be polite at all times.
- 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 as long as 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 Town Council deems to be unacceptable use of IT resources or system and behaviour by employees (this list not exhaustive).

- Allowing non-authorized users to access the internet or Council systems using the employees log in or while logged in.
- Visiting internet sites that contain obscene, hateful, pornographic or other illegal material.
- Using the Council's IT equipment to perpetrate any form of fraud.
- Using the Council's IT equipment to download, distribute or engage in the piracy of software, film, music or any other digital assets.
- Using the internet to send offensive or harassing material to other users.
- Downloading, copying, distributing or installing commercial software or any other copyrighted materials belonging to third parties, with the exception whereby such software is covered or permitted under a valid commercial agreement or other such licence.
- Hacking into or otherwise obtaining access to unauthorised areas of the Council's IT or database systems.

- Publishing defamatory and/or knowingly false material about the Council, its employees, members, colleagues and/or customers on social networking sites, 'blogs' (or other online journals), 'wikis' and any other online publishing format.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network.
- Gambling on-line.
- Disclosure of any confidential corporate information without express consent.
- Any other area that the Council reasonably believes may cause problems.

Social Media

1. Policy Statement

- 1.1 This section of the policy is intended to help employees and elected members make appropriate decisions about the use of social media such as social networking websites (e.g. Twitter, Facebook and LinkedIn), online forums, message boards, blogs or comments on web-articles, community websites or online newspapers.
- 1.2 This policy outlines the standards the Council requires employees and Council 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.

2. The Scope of the Policy

- 2.1 All employees and Council members are expected to comply with this policy at all times to protect the privacy, confidentiality and interests of the Council.
- 2.2 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.
- 2.3 Breach of this policy by Council members will be dealt with under the Code of Conduct.

3. Responsibility for Implementation of the Policy

- 3.1 The Council has overall responsibility for the effective operation of this policy.
- 3.2 The Council Manager is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our work.
- 3.3 All employees and Council members should ensure that they take the time to read and understand this policy. Any breach of this policy should be reported to the Council Manager or Chair of the Council.
- 3.4 Questions regarding the content or application of this policy should be directed to the Council Manager.

4. Using Social Media in General

- 4.1 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 Council members joining in and helping shape community conversation and direction through interaction in social media.
- 4.2 Before using social media on any matter which might affect the interests of the Council you must have read and understood this policy and;
- 4.3 Employees must have gained prior written approval to do so from the Council Manager.

5. Using Social Media Sites in the Name of the Council

- 5.1. The Council Manager and administration officers are permitted to post material on social media website(s) in the name of the Council and on its behalf in accordance with the rules and scope of this policy.
- 5.2 If you are not sure if any comments you are considering placing in the public domain are appropriate do not post them until you have checked with the Council Manager.

6. Rules for use of social media

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

- 6.1 Do not upload, post or forward a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- 6.2 Any employee/Council member who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague or a member of the general public onto a social media website should inform the Council Manager.
- 6.3 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 Council Manager or Chair of the Council.
- 6.4 Do not up load, post or forward any content belonging to a third party unless you have that third party's consent.
- 6.5 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.
- 6.6 When making use of any social media platform, you must read and comply with its terms of use.
- 6.7 Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of the Council.

- 6.8 It is important to be aware that you are personally responsible for content you publish onto social media or place into the public domain.
- 6.9 Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the 'temperature' and correct misrepresentations.
- 6.10 Don't discuss colleagues without their prior approval.
- 6.11 Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics or 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.
- 6.12 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.

7. Monitoring use of social media websites

- 7.1 Employees and Council members should be aware that any use of social media websites (whether or not 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.
- 7.2 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.
- 7.3 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 as appropriate (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.

- 7.4 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.

7.5 If you notice any use of social media by other employees/Council members in breach of this policy please report it to the Council Manager/Chair *in accordance with the Council's Whistle Blower Policy*.

8. Monitoring and review of this policy

8.1 The Council shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice.

9. References

Further information for Council members in the use of Social Media can be viewed online at:

<https://www.local.gov.uk/our-support/guidance-and-resources/comms-hub-communications-support/digital-communications-0>

i

ⁱAdopted by Council 27.11.18

Reviewed and amended 14.01.20

Reviewed and approved 23.02.2021