

Draft Computer and Phone Staff Acceptable Use Policy

Author: Louise Harrison, Town Clerk, Ferndown Town Council, 12 January 2021.

1. Purpose

1.1 The purpose of this policy is to ensure the proper use of Ferndown Town Council's (Council) computer and laptop, internet, email and telephone systems and make users aware of what Council deems as acceptable and unacceptable use of its communication systems.

It is accepted that a certain amount of time on the internet will be needed for employees to carry out their day-to-day work. However, it is stressed to employees with access to the internet that it should only be used for the purposes of official business of Council except as permitted below.

2. Requirements for use

2.1 The following rules must be adhered to by all users within Council.

It is prohibited to:

- send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks. If you receive an email of this sort, you must notify your line manager,
- forward a sensitive or controversial message without acquiring permission from the sender first,
- forge or attempt to forge email messages,
- disguise or attempt to disguise your identity when sending mail,
- access another employee's email unless:- (a) the employee has given their consent, (b) their email needs to be accessed by their line manager for specific work purposes whilst they are absent or (c) an appropriately authorised investigation is being undertaken,
- send email messages using other person's email address without permission. It should be stated in the message that you are the author of the message
- copy a confidential message or attachment belonging to another user without permission of the originator.

3. System monitoring

3.1 Whilst respecting the privacy of authorised users, under Data Protection legislation and Regulations, maintains its legal right to monitor and audit the use of email by authorised users under the Lawful Business Practice Regulations 2000 and GDPR 2018. Users expressly waive any right of privacy in anything they create, store, send or receive on Council's computer system. Council can, but is not obliged to, monitor emails without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, Council reserves the right to take appropriate disciplinary/legal action, which could result in termination of employment.

3.2 Users expressly waive any right of privacy in relation to any incoming or outgoing telephone calls made on the Town Council Offices telephone landline system. Council can, but is not obliged to, monitor all incoming or outgoing telephone calls.

4. Disclaimer

4.1 The following disclaimer will be added to each outgoing email:

'Disclaimer - You have received this email from Ferndown Town Council. The content of this email is confidential may be legally privileged and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

Ferndown Town Council ensures that email security is a high priority. Therefore, we have put efforts into ensuring that the message is error and virus-free. Unfortunately, full security of the email cannot be ensured as, despite our efforts, the data included in emails could be infected, intercepted, or corrupted. Therefore, the recipient should check the email for threats with proper software, as the sender does not accept liability for any damage inflicted by viewing the content of this email.

By contacting Ferndown Town Council you agree for your contact details may be held and processed for the purpose of corresponding.

You may request access to the information we hold on you, and to be removed as a contact at any time. To view Ferndown Town Council Privacy Notice visit www.ferndown.gov.uk'.

4.2 Council reserves the right to monitor, record and retain any incoming and outgoing emails for security reasons and for monitoring internal compliance with this policy. Although software may be used to check, monitor and/or block the contents of emails and attachments to identify the presence of malware; users are advised that they open any attachments at their own risk.

As a public body, Council may be required to disclose this email (or any response to it) under the Freedom of Information Act 2000 unless the information in it is covered by an exemption in the Act.

5. Personal use of Internet and email/social media

5.1 Subject to this policy, personal use could include but is not solely restricted to areas such as online banking, shopping, entertainment, leisure activities or bookings, personal research and web based email services (e.g. MSN and Hotmail). All such use is carried out at users' own risk and Council does not accept responsibility or liability for loss caused as a result of use of the internet.

Council permits discretionary use by employees of Council computers and laptops when authorised by the Town Clerk (in the case of the Town Clerk the Chairman of the Personnel Committee) free of charge to access the internet and send/receive email for personal/ developmental use. Employees authorised to use internet/email access for

personal purposes are deemed to have agreed to the following terms and conditions and only applies to times outside recorded working hours.

i. does not interfere with the performance of official duties;

ii. does not take a priority over work responsibilities;

iii. does not incur expense on the Council

iv. does not have a negative impact on the Council in any way, nor damage its reputation.

v. Unless specific prior permission from your line manager is granted, staff should not give their work email address as contact details for regular extra-curricular/social/voluntary commitments outside work.

vi. Any private research using the internet must be restricted to the employee's lunch time, rest period or break period as agreed by the line manager. Employees are not allowed to access social media websites for personal use from Council's computers or devices during working time and they must not be left running 'in the background', whilst at work. These provisions also apply to personal computers and mobile devices.

vii. Leaving social media sites 'running' constantly in work time is considered to be a breach of the acceptable use of the internet policy.

viii. Where it is essential to send an email (in staff own time) from work in relation to extra-curricular commitments, it must be prefaced with a disclaimer, making clear that Council is in no way connected to the content of the email. A 'Personal Disclaimer' must appear in: "This is a personal message from the sender, and no links with Ferndown Town Council are intended, nor should they be inferred".

ix. If staff have one-off social or non-work requirement to send an email from work (in their own time) i.e. chasing up a planning application, giving a reference for a friend, booking a venue etc, it must be prefaced with the Personal Disclaimer above, making it clear that the Council is in no way connected to the content of the email.

x. Do not use your work email address for any non-work communication if there is any possibility that the recipient will be influenced (either positively or negatively) by receiving a communication from an officer of the Council.

xi. To avoid cluttering the system with unwanted adverts or other material, please do not sign up for personal direct mail using your work email address. For example, if you have used the internet (in your own time) to buy goods or services, and are invited to subscribe to 'news of other products' please click 'no' or provide your home email address as the point of contact.

xii. Many people receive jokes or humorous articles from outside the organisation. Users must consider whether anyone is likely to take offence if you pass material on. Passing on offensive material via the work system is a disciplinary matter and may result in legal action or termination of employment.

xiii. Users are responsible for their individual accounts and as such they should take all reasonable precautions to prevent others from being able to use their account.

xiv. Do not send system account information by Email, this includes user accounts, passwords, internal network configurations, addresses or system names. This information is confidential.

xv. Users must not manually or automatically forward Council work related emails, that contains personal or sensitive (including commercially sensitive) information, to their own

personal/home email account, e.g. Gmail, Yahoo, Hotmail etc. This is strictly prohibited.

xvi. Should users have a legitimate business need to access work related emails and/or Council systems from home, remote access may be arranged formally subject to approval of the relevant business case by the user's line manager.

xvii. Before sending emails that contain personal information users must consider whether email is the most appropriate method of communication and ensure that the potential risks associated with emailing personal data e.g. email being sent to the wrong recipient or wrong attachment being sent is minimised.

xviii. Users access to, and the use of non endorsed "cloud storage & facilities" e.g. Dropbox & Google Docs, must be approved by the Town Clerk. For those facilities where approval has been granted, any use of such cloud facility must not be used for the purpose of storing or sharing confidential, personal or sensitive information.

xix. If you are informed of the presence of a virus, do not make colleagues aware by any electronic means, as by doing so you may inadvertently spread the virus. Contact the Town Clerk by telephone immediately in such circumstances.

xx. If users mistakenly access inappropriate information, they must immediately advise their Line Manager. This will protect them against any claim that they have intentionally violated this policy.

xxi. Users must promptly disclose to their line manager any messages or images they receive that are inappropriate or make them feel uncomfortable.

xxii. Use the "Out of Office Assistant" if you know you will not be able to access your Email system for a period of time. Good practice is to explain when you will be returning to work and whom the person can contact in your absence to deal with queries. Remember the Out of Office Assistant can be read by external organisations, so ensure your message is professional in its content.

xxiii. Using the council's computers or devices for playing games whether via the Internet or already on the system hard drive must be restricted to the employee's lunch time, rest period or break period as agreed by your line manager and they must not be left running 'in the background', whilst at work.

xxiv. Personal use of Council internet or phone systems must not incur any costs to the council. Council reserves the right to reclaim any charges incurred.

6. Listening to Music

6.1 Listening to music at work can only take place with the prior permission of the line manager regardless of the particular medium (radio, iPod, website, etc.) and regardless of whether the employee is using personal headphones.

Remember that the most important consideration is health and safety as Council must comply with its duty to take reasonable care of all employees' health and safety in terms of providing a safe working environment and safe working practices. Distraction to other employees and perception of a lack of professionalism by visitors is also a consideration.

6.2 If music is played openly in a public place (which also includes a workplace, even if the general public don't have access), whether this is on a radio, TV, CD or through the

internet, any organisation first needs to have obtained a licence from both the Performing Rights Society (PRS) and Phonographic Performance Ltd (PPL). Employees who want to listen to music on radios, the internet, etc. can therefore only do so on an individual basis via headphones, or to listen to their own personal music players when authorised by the Town Clerk.

7. Abuse of internet/email access

7.1 Any breach of this and related policies may warrant further investigation that may lead to the Council's Disciplinary Procedures being invoked and in certain circumstances, may necessitate the involvement of the Police.

7.2 The Council will co-operate fully with any audit or police investigation. If the investigation demonstrates that material that is accessed is offensive and/or illegal acts, or advocates discrimination to other people, this will be considered gross misconduct and appropriate disciplinary procedures will be followed, possibly resulting in dismissal.

7.3 Abuse of Internet/email access could include but is not exclusively:

- i. Accessing or distributing material that is profane or obscene (pornography), that incites illegal acts, violence or discrimination towards other people (hate literature).
- ii. Accessing web sites, blogs or chat rooms that are offensive, unsuitable or inappropriate to the workplace
- iii. Using language or behaviour likely to bring Council into disrepute
- iv. Using Council's official role/status for personal gain
- v. Using Council official role/status to support a specific political or issue-based campaign
- vi. Online gambling.
- vii. Using the equipment to contribute to fraud
- viii. Using or passing on privileged or confidential information
- ix. Making deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means (these actions are illegal).
- x. Harassing another person. Harassment occurs when a person engages in unwanted conduct which has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that person. If users are told by another person to stop sending them messages, they must stop. Further guidance on harassment is available through Council's Dignity at Work Policy.
- xi. Knowingly or recklessly posting false or defamatory information about a person or organisation.
- xii. Posting, forwarding or replying to chain letters or engaging in "spamming". (Spamming is the word used to describe the sending of annoying or unnecessary messages to a large number of people).
- xiii. Officers will not 'speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council), unless authorised to do so.
- xiv. The personal use of email or Internet access must be completely in accordance with this and any other Council policy.

8. Legal risks

8.1 Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. While email seems to be less formal than other written communication, the same laws and guidelines apply.

Users should note that an email has the same significance and legal implications as a signed letter. Furthermore, users should never send 'off the record' emails – nothing is 'off the record' where the law requires disclosure of information.

Users should be aware of the legal risks of email:

- If you send or forward emails with any libellous, defamatory, offensive, racist or obscene remarks, both you and Council can be held liable. In addition, it may be considered to have been an infringement of the disciplinary procedure.
- If you unlawfully forward confidential information, you and Council can be held liable.
- If you unlawfully forward or copy messages without permission, you and Council can be held liable for copyright infringement.
- If you knowingly send an attachment that contains a virus, you and Council can be held liable.

8.2 Whilst it can sometimes be helpful to maintain a chain of e-mails on a particular subject, long chains of e-mails are best avoided. Information from emails may be required to answer Data Protection/FOI requests and difficulties can arise if a chain of e-mails refers to data which should not be disclosed. Users should consider this when responding to or creating an e-mail chain and, where appropriate, create a fresh message.

8.3 Read and delete emails regularly. Unless notification has been made by an "out of office" message emails should be responded to within 3 working days. Keep your 'Inbox', and 'Sent' folder contents to a minimum. Regularly delete 'Deleted items' and associated sub-folders.

8.4 Please follow the guidelines in this policy to minimise the legal risks to yourself and Council. If any user disregards the rules set out in this policy, the user will be fully liable and Council will disassociate itself from the user as far as legally possible.

8.5 Users should be aware of UK and international laws that govern the use of emails. These include any statutory modifications or amendments but are not limited to:

- Copyright
- Libel and Defamation
- Public Records Acts 1958 and 1967
- Data Protection Act 1998 and GDPRs 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Electronic Commerce (EC Directive) Regulations 2002

9. Access to systems (general)

9.1 Should any employee attempt to gain access to a system for which they do not have authority, they will be acting in breach of the Computer Misuse Act 1990. This will be regarded as gross misconduct and the disciplinary procedure will be invoked.

9.2 Employees are reminded that the Computer Misuse Act 1990 specifies the

following as criminal offences:

- unauthorized amendment or damage to data.
 - unauthorized access, or contact with other systems, with criminal intent.
- 9.3 Any employee found to be attempting to gain unauthorised access to any internal mailbox without authority will also be subject to disciplinary procedure.
- 9.4 All PCs are virus protected and virus shields updated regularly.
- 9.5 All PCs are provided with a spam filter which can be updated regularly.
- 9.6 Only DVD/CDs/Portable Device provided by Council are to be used in any workstation, without specific authority.
- 9.7 Employees must gain authorisation from the Town Clerk before installing any software onto the Council IT system.
- 9.8 Any software provided by Council can only be removed with specific authority.

10. Unsolicited communications

10.1 No employee can be held responsible by Council for the contents of any unsolicited communication, regardless of its contents, when received through any systems operated and maintained by Council.

11. Telephone system

- 11.1 Council employees must not use Council's telephone system for personal use, except in emergencies.
- 11.2 This includes any mobile telephone or similar device provided by Council.

12. Personal telephones / hand held devices

12.1 Use of personal telephones / handheld devices in working hours is discouraged, other than in an emergency. Excessive use could be subject to disciplinary action.

13. Social media

13.1 This policy does not include guidance on the acceptable use of social media such as blogs, message boards, social networking (Facebook, Twitter, LinkedIn, My Space) and content sharing websites (Flickr, Youtube) for Council business (see Council's Social Media Policy).

.