PEMBROKE TOWN COUNCIL

Pembroke Town Council IT Policy

1. Introduction

Pembroke Town Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

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

2. Scope

This policy applies to all individuals who use Pembroke Town Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Pembroke Town Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Pembroke Town Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

All sensitive and confidential Pembroke Town Council data should be stored and transmitted securely using approved methods. Regular data backups should be

performed to prevent data loss, and secure data destruction methods should be used when necessary.

6. Network and internet usage

Pembroke Town Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Pembroke Town Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

Pembroke Town Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

9. Mobile devices and remote Work

Mobile devices provided by Pembroke Town Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

10. Email monitoring

Pembroke Town Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

13 Training and awareness

Pembroke Town Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

14. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

15. 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.

16. Contacts

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

All staff and councillors are responsible for the safety and security of Pembroke Town Council's IT and email systems. By adhering to this IT and Email Policy, Pembroke Town Council aims to create a secure and efficient IT environment that supports its mission and goals.

Date: _____

Signature: _____

Role: _____

PEMBROKE TOWN COUNCIL
Social Media Policy

Introduction

The world is experiencing the biggest ever change in how information is created and owned, as well as the speed in which it can be shared. This is changing the way we live, work and even how we speak and think.

Social media is a blanket term applied to a range of online multimedia tools that are used for creating content and two-way communication. They can be accessed via your smartphone, PC, laptop, tablet or smart TV. All social media accounts are free of charge and can be set up quickly and easily from an Internet page.

1. Policy Statement

1.1. This policy is intended to help employees and elected members 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.

1.2. 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.

2. The Scope of the policy

2.1. All employees and elected 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 elected 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 Clerk 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 elected members 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.
3.4. Questions regarding the content or application of this policy should be directed to the Clerk.

4. Using social media sites in the name of the council

4.1. The Clerk and elected members 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.
4.2. If you are not sure if your comments are appropriate do not post them until you
have checked with the Clerk/Chair.

5. Using social media

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

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/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/Chair.
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 Clerk/Chair.
6.4. Do not upload, 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. You are personally responsible for content you publish into social media tools.
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 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.
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 elected 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 (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); or

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/elected members in

breach of this policy please report it to the Clerk/Chair *in accordance with the Council's Whistle Blower Policy.*

8. What to bear in mind

When you engage with people online it is important that a common sense approach is taken, to include trying to verify that the person you are correspondence with is as you are being led to believe before replying. The things that can get you into hot water anywhere else are just the same things to avoid in social media. It is important that you think before you post online and check for accuracy of the content as wors cannot be unspoken. Even if you delete a statement, blog or tweet, it will probably already have been read, indexed or duplicated in places beyond your reach. Care should also be taken when, linking, sharing, or re-tweeting content where this could be perceived as endorsement of the content. You should think about your digital footprint, which is a term used to describe the entirety of information that you post online, including photos and status updates. Criminals ca use this publicly available information to steal your identity or use it to make phishing messages more convincing. The law of defamation applies to social media in the same way as written or spoken communication. **You can be sued for damages if a person or business considers their reputation has been or may be harmed because of your actions.** You need to be clear at all times whether you are posting in a personal or a professional capacity, as an elected member or private individual. Including Cllr or Councillor in a name may give the impression and so lead to a conclusion that the councillor is writing in the capacity as an elected member. Anyone receiving threats, abuse or harassment via their use of social medial should report it to their political group leader, members services and/or the police. Complaints can also be made following the social media provider's own policies..

9. Monitoring and review of this policy

9.1. The Council shall be responsible for reviewing this policy to ensure that it meets
legal requirements and reflects best practice.
Further information for elected members, published by the Welsh Local Government
Association, on the use of social media can be viewed on the One Voice Wales website:-
http://www.onevoicewales.org.uk/OVWWeb/good_practicegeneral-8204.aspx
Reviewed and adopted:
Review date: