Pembroke Dock Town Council

Internet & Email usage policy

Use of both the internet and email has increased for the Town Council and council needs to ensure that it is used for the benefit of the Council and to minimize any risks. This is done by introducing an acceptable use policy (which is adhered to by everyone within the Council). Communications via email, and internet usage undertaken in the name of the Council or on Council systems carry inherent risks including potential defamation, the spreading of viruses, including Trojans which can steal data, 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.

At the same time, Councils' right to monitor email and internet usage has to be done in accordance with the law, in particular the Data Protection Act 1998 and the Human Rights Act, as monitoring is usually intrusive and employees have a right to some privacy within the workplace.

1. **Policy Coverage**

   This Policy makes it clear that the Council provides employees with email and internet access as required for the performance and fulfilment of job responsibilities and that therefore usage should be restricted to these activities. Employees are prohibited from using their own personal devices or software on Council owned systems, due to the risk of virus spreading.

   Council will allow access to the internet or to email via the Council's systems for non-work related purposes. Examples of non-work related activities are, but not limited to, Internet Banking, travel arrangements, weather forecasting etc. Employees must exercise their sensible judgment in these matters. Occasional and reasonable personal use of the Council's internet and email service is permitted, provided that this does not interfere with work performance or security.

2. **Monitoring and Privacy Issues**

   The Data Protection Act does not prevent monitoring of emails and internet usage but it does set out principles for the gathering and use of personal information.

   Care must be taken regarding monitoring private emails, for example in relation to occupational health or emails between an employee and their trade union representative. Care therefore needs to be taken when monitoring if emails are clearly personal and such clearly personal emails should not be opened.

   Councils are subject to Article 8 of the Human Rights Act. This creates a right to respect for private and family life, and therefore Council needs to take care to ensure that any monitoring is not excessive.

   Council should also warn the employee that if monitoring identifies potential breaches of the Policy this may lead to formal disciplinary action and make it clear that serious breaches may amount to summary dismissal for gross misconduct.

3. **Email Etiquette**

   It is important to set the parameters in relation to email usage. Such guidance includes:

- Agreed email signatures;
- Appropriate business language;
- Waiver clauses at the end of each email message;
- Prohibition on circulating offensive, indecent or obscene material or anything which breaches the Equal Opportunities Policy;
- Rules regarding confidentiality
- Dealing with attachments and size of documents;
- How much personal email is acceptable;
- Double checking the recipient's address is correct;
- Checking whether applying "to all" is appropriate;
- Guidance on saving, filing and photocopying emails.

4. Unacceptable behaviour on the Internet

This Policy sets out what is deemed unacceptable use or behaviour by employees and this includes:

- 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 otherwise 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, your colleagues and/or our 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 on-line;
- disclosure of any confidential corporate information without express consent;
- any other area that the Council reasonably believes may cause them problems

5. Social Media

Employees are to be made aware that entries entered on such media which have a detrimental impact on the Council or colleagues may lead to formal disciplinary action. They should also be prohibited from naming the Council they are employed by on such sites or discussing internal council matters on such sites. Accessing such sites for personal use is also prohibited during working hours.

6. Consequences of Breaches.

Council policies make it clear the potential consequences of breaching their rules on email and internet usage. If an offence is very serious, it is clear that serious breaches may be treated as gross misconduct. Apart from disciplinary action this could include withdrawing access to the internet for private purposes during work time.