PEMBURY PARISH COUNCIL

Working for Pembury People

IT Policy

Adopted 15/05/2023

Version:	Date Approved:	Review Date:
1.0	15/05/2023	01/07/2025

1. Introduction

1.1. This policy has been adopted by the Parish Council ("Council") in order to:

1.1.1. prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material).

1.1.2. protect confidential, personal or commercially sensitive data.

1.1.3. prevent the introduction of viruses.

1.1.4. prevent the use of unlicensed software.

1.1.5. ensure that Council property is properly looked after.

1.1.6. monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse.

1.2. The consequences of misuse can be severe. Examples of potential damage include, but are not limited to, malware infections, legal and financial penalties for data leakage and lost productivity from network downtime.

1.3. The Council provides Councillors and employees with access to various computing and telephone communication methods ("facilities") to allow them to undertake the responsibilities of their position and to improve internal and external communication.

2. Scope

2.1. This policy sets out the Council's position on the use of the facilities and it includes:

2.1.1. Employees and Councillors' responsibilities and potential liability when using the facilities.

2.1.2. the monitoring policies adopted by the Council; and guidance on how to use the facilities.

2.2. This policy has been created to:

2.2.1. ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring

2.2.2. protect the Council from the risk of financial loss, loss of reputation or libel; and

2.2.3. ensure that the facilities are not used so as to cause harm or damage to any person or organisation.

2.3. This policy applies to the use of:

2.3.1. local, inter-office, national and international, private or public networks and all systems and services accessed through those networks.

2.3.2. desktop, portable and mobile computers and applications owned or leased by the Council.

2.3.3. social media; and

2.3.4. electronic mail and messaging services.

3. Breach of the Policy

3.1. In respect of employees, breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's disciplinary process.

3.2. Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal grievance procedure.

4. Email (Internal or External Use)

4.1. All Councillors and relevant employees will be issued with a Council email account which must always be used when transacting on behalf of the Parish Council. Such account will only be used for Council correspondence.

4.2. Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should either, be sent using password protected attachments or by using a password protected link to documents in SharePoint.

4.3. Email should be treated as any other documentation. If you would normally retain a certain document in hard copy, you should retain the email.

4.4. Do not forward email messages unless the original sender is aware that the message may be forwarded and that the whole email chain has been checked for appropriate content. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

4.5. It is good practice to copy and paste information from an email to pass it on, rather than forwarding on an email, in order to remove the IP address from the header.

4.6. Personal emails are subject to Freedom of Information requests/subject access requests, if they relate to Council business or an individual and it is a criminal offence to block the release of data.

4.7. Council emails should not be forwarded to a personal account without the Data Controller's permission and doing so is a breach of the Data Protection Act and Computer Misuse Act.

4.8. Your email inbox should be checked for new emails on a regular basis.

4.9. As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

4.10. Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of an email account is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

4.11. Councillors and employees will be required to surrender their email account and all of its contents to the Clerk when they leave the Council. The Clerk on leaving the Council needs to do the same, but to the Chair of the Parish Council.

5. Laptop computers, PC's, tablets and smart phones

5.1. Laptop computers, PC's, tablets and smart phones belonging to the Council along with related equipment and software are subject to all of the Council's policies and guidelines governing non-portable computers and software). All laptops, PC's and tablets will be encrypted.

5.2. When using such equipment:

5.2.1. you are responsible for all equipment and software until you return it. It must be kept secure at all times.

5.2.2. The Clerk and the individual employees or Councillor are the only persons authorised to use the equipment and software issued to that employee or Councillor.

5.2.3. Every employee or Councillor must work within the Councils filing/software environment when carrying out Council business to ensure that all data is backed up and accessible by the Clerk.

5.2.4. if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention, initially through the Clerk or in their absence, the Deputy Clerk.

5.2.5. upon the request of the Council at any time, for any reason, you will immediately return any equipment and all software to the Council.

5.2.6. Software piracy could expose both the Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licences to which the Council is a contracting party. This means, that:

5.2.6.1. software must not be installed onto any of the Council's computers unless this has been approved in advance by our IT Contractors or Council. They will be responsible for establishing

that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities.

5.2.6.2. software should not be removed from any computer, nor should it be copied or loaded on to any computer without prior consent.

5.2.7. If you are using your own laptop or PC to connect with the Council's network or to transfer data between the laptop or PC and any of the Council's computers you must ensure that you have obtained prior consent, comply with instructions and ensure that any data downloaded or uploaded is free from viruses.

5.2.8. In order to maintain the confidentiality of information held on or transferred via the Council's equipment, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Council's equipment/network. This will be changed regularly and must be kept secure and not shared with anyone. A full list of account details should be held with the Clerk in a sealed secure unit.

5.2.9. You are expressly prohibited from using the equipment for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council or its clients other than in the normal and proper course of carrying out your duties for the Council.

5.2.10. In order to ensure proper use of Council computers, you must adhere to the following practices:

5.2.10.1. anti-virus software must be kept running at all times.

5.2.10.2. media storage such as USB drives, CD's or portable hard drives will not be permitted unless they have been provided by the IT supplier or approved by Council.

5.2.10.3. obvious passwords such as birthdays and spouse names, etc, must be avoided (the most secure passwords are random combinations of letters and numbers).

5.2.10.4. all files must be stored on the network/computer cloud drive which is backed up regularly to avoid loss of information.

5.2.10.5. always log off the computer/network before leaving your computer for long periods of time or overnight.

6. Internet

6.1. Posting information on the internet, whether on a newsgroup, via a chat room or via email is no different from publishing information in the newspaper. In the ordinary course of things, the Clerk is the only person authorised to make such postings or to authorise others to do so on their behalf.

6.2. Using the internet for the purpose of trading or carrying out any business activity other than Council business is strictly prohibited.

6.3. For the avoidance of doubt the matters set out above include use of wireless facilities.

7. Monitoring Policy

7.1. The policy of the Council is that we may monitor your use of the equipment.

7.2. The Council recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the equipment.

7.3. The Council may from time to time monitor the equipment. Principal reasons for this are to:

7.3.1. detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies.

7.3.2. ensure compliance of this policy.

7.3.3. detect and enforce the integrity of the equipment and any sensitive or confidential information belonging to or under the control of the Council.

7.3.4. ensure compliance by users of the equipment with all applicable laws (including data protection), regulations and guidelines published and in force from time to time.

7.3.5. monitor and protect the wellbeing of employees and Councillors.

7.4. The Council may adopt at any time a number of methods to monitor use of the Facilities. These may include:

7.4.1. recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content.

7.4.2. recording and logging the activities by individual users of the Facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the internet and websites visited.

7.4.3. physical inspections of individual users' computers, software and telephone messaging services.

7.4.4. periodic monitoring of the Facilities through third party software including real time inspections.

7.4.5. physical inspection of an individual's post.

7.4.6. archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.

7.5. The Council will not (unless required by law):

7.5.1. allow third parties to monitor the Facilities (with the exception of our appointed IT supplier); or

7.5.2. disclose information obtained by such monitoring of the Facilities to third parties unless the law permits.

7.6. The Council may be prohibited by law from notifying employees using the equipment of a disclosure to third parties.

8. Social Media

8.1. The Council may use social media to communicate messages to residents and will only be used:

8.1.1. by the Clerk and persons authorised by the Clerk.

8.1.2. to transmit factual information and news, not personal opinion.

8.1.3. to respond to comments and requests submitted via the account.

8.2. Employees and Councillors using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of the Council.

9. General guidance

9.1. Never leave any equipment or data (including client files, laptops, computer equipment and mobile phones) unattended on public transport or in an unattended vehicle.

9.2. Observation of this policy is mandatory and forms part of the terms and conditions of employment of employees and the terms of access to the Council's systems and offices. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

9.3. Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be taken with these devices: sensitive information should be stored in password protected or encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

9.4. All workstations (desktops and laptops) must be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

9.5. Any documents downloaded to a laptop or tablet must be deleted after use and stored in the Council's cloud software only.

10. 'Bring Your Own Device'

In this policy:

10.1. 'Devices' means computers (desktop and laptop), tablets, smartphones and external hard drives.

10.2. 'Council Business' means any activity undertaken in the role of Councillor or employee of the Council.

10.3. 'Personal Data' has the meaning set out in Article 4(1) of the General Data Protection Regulation:

10.4. "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

10.5. 'Personally owned' means ownership of a Device by a person or legal entity which is not the Council.

11. Purpose

11.1. The purpose of this policy is to ensure so far as possible that personally owned Devices used by Councillors and employees to conduct Council Business are used in a manner which protects Personal Data.

12. Risks

12.1. The Council has identified the following risks inherent in using personally owned Devices to conduct Council Business:

Event / Action	Risk
Inadequate or lack of appropriate security measures used to control access to Device	Personal Data may be accessible to third parties
Device used in an insecure manner	Device could be affected by malware which could result in Personal Data being accessed by third parties
Device lost or stolen	Personal Data may be accessible to third parties
Device sold or given away	Personal Data may be accessible to third parties unless Device

	appropriately cleared before transfer by restoring factory settings
Employees cease to be employed by the Council or Councillor ceases to be a member of the Council	Personal Data may remain accessible via the Device and could be used for unauthorised purposes or disclosed to third parties

13. Access to Devices

13.1. Devices used for Council Business must be secured by a password or a biometric access control such as fingerprint recognition.

13.2. Devices must have appropriate and up to date anti-virus and anti-malware software.

13.3. Home Wi-Fi networks must be encrypted.

13.4. Care should be exercised if using public Wi-Fi to connect Devices.

13.5. Passwords must comply with the following rules:

13.5.1. Password management software or a secure written system should be used to store passwords.

13.5.2. A different strong password should be used for each and all Devices or email accounts.

13.5.3. Passwords must not be disclosed to any other person. If a password is disclosed to any other person, whether deliberately or inadvertently, it must be changed immediately.

13.5.4. Passwords should comprise a mix of letters, numbers and symbols, at least 12 characters long.

13.6. Devices must be configured to automatically lock if left idle for more than five minutes in the case of smartphones, tablets or laptops and ten minutes in the case of desktop computers.

14. Retention and Use of Personal Data

14.1. Personal Data received for the purposes of Council Business and accessed via a personally owned Device must be permanently deleted from the Device or email account once the related Council Business is completed.

14.2. Personal Data should not be retained on a Device or in an email account in case it is needed for a different purpose in the future unless permission has been obtained to retain the data for general Council Business or unless the Council is required by law to retain the Personal Data.

14.3. Personal Data must not be used by any person for any other purpose than that for which it has been provided.

14.4. Personal Data received for the purposes of Council Business must not be shared with any other person or organisation.

15. Lost or Stolen Devices

15.1. In the event that a Device is lost or stolen, or is suspected of having been lost or stolen, the Chairman and Clerk of the Parish Council must be informed. The Council will work with the owner of the lost or stolen Device to identify any personal data at risk and will then take appropriate action, including reporting any breach to the ICO as necessary.

16. Repair of Devices

16.1. If a Device needs to be repaired, the owner will take all reasonable steps to ensure that the repairer cannot access any Personal Data.

17. Transfer or Disposal of Devices used for Parish Council Business

17.1. If the owner wishes to transfer or dispose of a Device which has been used for Council business, all Personal Data must be deleted from that Device using a method which prevents recovery. Any email accounts used by the Councillor or Clerk for Council Business should be deleted from the Device.

18. Leaving the Parish Council

18.1. If a Councillor ceases to be a member of the Council for any reason:

18.1.1. all Personal Data received in the course of Council Business must be permanently deleted from Devices and from any email account used for Council Business; and

18.1.2. all hard copies should be shredded or passed to the Clerk for destruction

18.2. On the termination of employees' employment by the Council:

18.2.1. employees must return Devices issued by the Council immediately; and

18.2.2. all Personal Data or other information received in the course of Council Business must be permanently deleted from personally owned Devices.