WOULHAM PARISH COUNCIL - IT Policy 2025

Communications via email, internet and utilisation of IT Infrastructure are adopted universally in everyday life. With familiarity comes risk, and business undertaken in the name of the Council or on Council systems must be protected from the consequences of misuse or abuse, which can be severe. This policy identifies the principal matters which affect Wouldham Parish Council and identifies practices and processes which should be adhered to by Councillors and staff members when undertaking Council Business.

1. Introduction

In respect of minimising reputational harm, data loss, financial loss, legal breach or loss of operational capacity, this policy has been adopted by Wouldham Parish Council ("WPC") to:

- prevent inappropriate use of Council IT infrastructure causing harm or damage to any person or organisation (including personal use or for accessing and circulating pornographic, racist, sexist or defamatory material).
- protect confidential, commercially sensitive or personal data.
- prevent the introduction of software viruses.
- prevent the use of unlicensed software.
- prevent insecure and unauthorised use of IT infrastructure.
- ensure that Council property is properly secured and looked after.
- ensure that electronic documents are securely retained.
- monitor computer use to ensure compliance with internal policies and rules and to detect abuse.
- control unscrutinised use of AI technologies and incorrectly interpreted internet data.
- establish procedures for device disposal or loss.

2. Scope

This policy should be read in conjunction with other WPC operational Policies; in particular the Social Media Policy; the General Privacy Notice and the Document retention policy

The Council provides Councillors and employees with access to various IT infrastructure and telephone communication methods ("Facilities") to allow them to undertake the responsibilities of their position and to facilitate internal and external communication.

This policy sets out the Council's position on the use of the Facilities and personal IT infrastructure and includes:

- Staff member responsibilities and potential liability when using the Facilities.
- Councillor obligations.
- Use of personal IT infrastructure by either Councillors or staff members.
- The monitoring policies adopted by the Council.
- Guidance on how to use the Facilities.

This policy applies to the use of:

- Local, inter-office, national and international, private or public networks and all systems and services accessed through those networks.
- Desktop, portable, mobile computers, and software applications.
- Social media.
- Electronic mail and messaging services.
- Mobile telephones.

3. Breach of the Policy

- In respect of staff members, breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's formal disciplinary process.
- In respect of Councillors, breach of this policy will be dealt with by reference to the WPC Code of Conduct.
- Any person 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. Computer Facilities: Secure Use of Computer Systems

Subject to anything to the contrary in this policy the Facilities must be used for Council business purposes only. It is expressly prohibited to use the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council other than in the normal and proper course of carrying out duties for the Council.

Staff members must not use their own personal IT equipment to carry out any duties for the Council, unless specifically authorised in writing by the Charman. In order to ensure proper use of Council IT infrastructure, the following practices must be adopted:

• anti-virus software must be kept running at all times.
• except the clerk, media storage such as USB drives, or portable hard drives will not be permitted
• a log-on ID and password is required for access to the Council's network. This will be changed regularly and must be kept secure and not shared with anyone.
• other devices must be secured with passwords, which should not be obvious such as birthdays, familiar names or similar (the most secure passwords are random combinations of letters and numbers).
• passwords set-up or changed on devices by individual users must be notified to the Clerk for secure retention.
• all data files must be stored on the Council network drive.
• always log off the network before leaving a computer for long periods of time or overnight.
• never leave any equipment or data (including documents, laptops, computer equipment and mobile phones) unattended in a public place, on public transport or in an unattended vehicle.
• if a Councillor uses their IT equipment or to transfer data between their equipment and any of the Council's computers, prior consent must be obtained from the Clerk, with measures adopted to ensure that any data downloaded or uploaded is free from viruses. (see paragraph 12).

5. Computer Facilities: Software

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:

• software must not be installed onto any of the Council's computers or devices unless this has been approved in advance by the Clerk. 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.
• software should not be removed from any computer, nor should it be copied or loaded on to any other computer or device without prior consent of the Clerk.
• AI technologies should not be used in the preparation of any Council business

6. Computer Facilities: Responsibility for and care of IT infrastructure

Laptop computers and smart phones belonging to the Council along with related equipment and software are subject to this policy whether being used by a member of staff or any Councillor. When using such equipment:

• the nominated user is responsible for all equipment and software until it is returned and must be kept securely.
• the nominated user is the only person authorised to use the equipment and software issued to them.
• if the nominated user discovers any mechanical, electronic, or software defects or malfunctions, they should immediately bring such defects or malfunctions to the Council's attention.
• upon the request of the Council at any time, for any reason, the nominated user must immediately return any equipment and all software to the Council.

7. Email (Internal or External Use)

All Councillors and staff members will be issued a Council email account which should be used when transacting on behalf of the Parish Council. All are not permitted to forward Council emails to personal email accounts. All 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.

Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything that may not usefully be made public, and adhere to the following:

• Email should be treated as any other documentation. If a certain document would normally be retained in hard copy, the email should be retained.
• do not forward email messages unless the original sender is aware that the message may be forwarded. Always check any confidentiality notice at the end of emails.
• as with any communications, the high standards expected by the Council should be maintained, and nothing said that might appear inappropriate or that might be misinterpreted by a reader.
• be careful what is written and never forget that email and written correspondence are not the same as conversation: emails are a written record which can be duplicated at will and may be subject to the Freedom of Information Act
• refer also to the WPC Social Media Policy.

8. Internet and Council Website

Posting information on the internet, whether on a Facebook, WhatsApp, or via email, is no different from publishing information in a newspaper. The Clerk is the only person authorised to make postings to the internet or to the Council website. The Clerk may however authorise others to do so on their behalf.

9. Social Media

The Council uses a dedicated web page and Facebook to communicate messages to residents and will only be used:

- by the Clerk and persons nominated by the Clerk.
- to transmit factual information and news, not personal opinion.
- to respond to comments and requests submitted via the account.

The Council does not use any other forms of social media. Councillors and staff members using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of the Council. Refer also to the WPC Social Media Policy.

10. Monitoring

The policy of the Council is that it may monitor use of the Facilities by either Councillors or staff members.

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 Facilities. The Council may from time to time monitor the Facilities in order to:

- 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.
- ensure compliance of this policy.
- detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Council.
- ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time.
- monitor and protect the wellbeing of employees. The Council may adopt at any time several methods to monitor use of the Facilities.

These may include:

- 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.
- physical inspections of nominated user' computers, software and telephone messaging services.
- periodic monitoring of the Facilities through third party software including real time inspections.
- reviewing and logging of internal, inter-office and external telephone calls made or received by employees using Council mobile telephones. Such logs may include details of length, date and content.
- physical inspection of an individual's post.
- archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.

The Council will not (unless required by law):

- allow third parties to monitor the Facilities (except for any appointed IT supplier);
- disclose information obtained by such monitoring of the Facilities to third parties unless the law permits. The Council may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

11. Personal Data, Data Retention and Storage

Refer to the WPC General Privacy Notice.

Refer to the WPC Data Retention Policy

12. Councillors using their Own Devices

Staff members must not use their own personal IT equipment to carry out any duties for the Council, unless specifically authorised in writing by the Charman.

Councillors are not customarily provided with any IT equipment to assist with carrying out their Council duties. So far as is practicable, to ensure that personally owned devices used by Councillors are used in a manner that protects Personal Data and to maintain consistency with other provisions of this policy, the following elements of good practice should be observed.

12.1. Safe Usage of Devices

• devices used for Council Business must be secured by a password or a biometric access control, such as fingerprint recognition.
• passwords should not be obvious such as birthdays, familiar names or similar (the most secure passwords are random combinations of letters and numbers).
• different passwords should be used for each device or email account and not be disclosed to any other person.
• passwords should be changed at least every 12 months.
• devices used by one or more persons must have a separate password protected user profile for the Councillor, which cannot be accessed by any other person.
• devices should be configured to automatically lock if left idle for more ten minutes.
• devices must have appropriate and up-to-date anti-virus and anti-malware software.
• home Wi-Fi networks should be password protected and care should be exercised when using public Wi-Fi to connect devices.

.12.2. Retention and Use of Personal Data

• 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. It should not be retained on a device or in an email account in case it is needed for a different purpose in the future.
• Personal Data must not be used by any person for any other purpose than that for which it has been provided.
• Personal Data received for the purposes of Council Business must not be shared with any other person or organisation.
• refer also to the WPC General Privacy Notice.
• a full set of Council passwords shall be printed and passed to the Chairman in a sealed envelope, only to be opened in case of emergency and if the Clerk is not available. To be updated when required.

12.3. Replaced, Repaired, Lost or Stolen Devices

• if a Councillor wishes to transfer or dispose of a device that has been used for Council Business, all Personal Data must be deleted from that device using a method that prevents recovery.
• any email accounts used by the Councillor for Council Business should be deleted from the device.
• if a device used to transact Council Business needs to be repaired, the Councillor must take all reasonable steps to ensure that the repairer cannot access any Personal or Council Data.
• in the event that a device used to transact Council Business is lost or stolen, or is suspected of having been lost or stolen, the Chair and Clerk of the 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.

12.3. Leaving the Parish Council

• if a Councillor ceases to be a member of the Council for any reason, all Personal and Council Data received in the course of Council Business must be permanently deleted from every personal device used by a Councillor to transact Council Business.
• any email account and associated mailbox files used for Parish Council Business must be deleted.
• all hard copies of any email or document should be shredded or passed to the Clerk for destruction.

This policy has been approved and adopted by Wouldham Parish Council at a Full Council Meeting held on:

_____

Chair: _____ Date: