COMPTON PARISH COUNCIL

EMAIL AND INTERNET USAGE POLICY

Introduction

The Parish 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.

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well- defined policy helps to:

- Set expectations for appropriate use of equipment and systems.
- Raise awareness of risks associated with IT use.
- Safeguard the council's data and digital assets.
- Clarify what constitutes acceptable and unacceptable use.
- Outline the consequences of policy breaches.

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address.

Scope of this Policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part- time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer Use

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes; however reasonable personal use is permitted (reasonable interpreted as in the opinion of the clerk).

1.1.2 All computer and other electronic equipment supplied should be treated with good care at all times.

1.1.3 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Clerk.

1.1.4 Any faults or necessary repairs must be reported to the Clerk.

Equipment

2.1 Portable Equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended and should never be left in parked vehicles or at any council or non-council premises.

2.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code.

2.1.5 If an item of portable equipment is lost or damaged this should be reported to the Clerk.

2.1.6 Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.2 Use of Own Devices

2.2.1 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's network or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in

commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.
2.2.2 However, the same security precautions apply to personal devices as to the council's equipment. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.
2.2.3 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy.
2.2.4 In cases of legal proceedings against the council or external stakeholders, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.
2.2.5 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.
2.2.6 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a strong password. For smartphones and tablets this should lock the device after three failed login attempts.
- configure their device(s) to automatically prompt for a password after a period of inactivity.
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email);
- ensure secure WiFi networks are used.
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device.
- inform the clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources.

2.2.7 Personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen.

2.2.8 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements.
2.2.9 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.
2.2.10 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow the IT provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.
2.2.11 Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment.

3.1 Password and Authentication Policy
3.1.1 All user accounts must be protected by strong, secure passwords.
To further strengthen account security:
• Initial user account passwords must be generated by the IT provider.
• Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
• Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
• The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.
3.1.2 Access to Passwords
• Passwords are personal and must not be shared under any circumstances.
• Only the assigned user of an account may access or use the associated password.
• Administrative credentials must be stored securely and only accessible to authorised personnel.
3.1.3 Password Storage and Management
• Passwords must not be stored in plain text or written down in insecure locations.
3.1.4 Password Change Requirements
• Immediately change password if compromise is suspected.
3.1.5 Responsibility
• Users are responsible for creating and maintaining secure passwords for their accounts.

4.1 Monitoring

4.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.
in place.

4.1.2 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

4.1.3 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy.

4.1.4 All computers will be periodically checked and scanned for unauthorised viruses.

5.1 Remote working

5.1.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, or at external stakeholder's premises or any other different venue), as follows:

• if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used.
• the location and direction of the screen should be checked to ensure confidential information is out of view.
• any data printed should be collected and stored securely.
• all electronic files should be password protected and the data saved to the council's system/services when accessible.
• papers, files or computer equipment must not be left unattended
• any data should be kept safely and should only be disposed of securely.
• papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car.

6.1 Email

6.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Councillors, staff, and other

authorised users need to be careful not to introduce viruses onto council systems.
6.1.2 All councillors, staff, and other authorised users who need to use email as part of their role will be given their own council email address and account.
6.1.3 Email messages sent on the council's account are for council use only. Personal use is not permitted.

7.1 Use of the Internet
Copyright
7.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software.
7.1.2 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied.
7.1.3 A website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1 Network and Internet Usage
8.1.1 Staff members are encouraged to use the internet responsibly as part of their official and professional activities.
8.1.2 Information obtained via the internet and published in the name of the Council must be corroborated as accurate and valid according to recognised government, educational, or standards of UK Publishing regulations.
8.1.3 Information obtained via the internet and published in the name of the Council must be relevant and professional. A disclaimer must be stated where personal views are expressed.
8.1.4 The use of the internet to access and/or distribute any kind of offensive material will not be tolerated.

9.1 Use of social media
9.1.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.
9.1.2 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and

enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable. However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced.

Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

9.1.3 To protect both the council and its interests, all are required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

• Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.

• Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own.

• Any employee who is developing a site or writing a blog that will mention the council, must inform the clerk that they are writing this and gain agreement before going 'live'.

• The council expects councillors, staff, and other authorised users to be respectful about the council and its current or potential e.g. all staff, including employees, councillors, clerks, and authorised users and not to engage in any name calling or any behaviour that will reflect negatively on its reputation

• Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.

• Inappropriate conversations with external stakeholders should not take place on any social networking sites, including forums.

• Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an

online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles.
• Contacts by the media relating to the council should be referred to the clerk.
• Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
• During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. All such contacts will be considered council property and may be subject to disclosure upon request.
9.1.5 External stakeholders contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data including external stakeholders contact details from any personal device/equipment.

10.1 Reporting and Sanctions
All suspected security breaches or incidents should be reported immediately to the Clerk. Any email-related security incidents or breaches should be reported to the Clerk immediately.
10.1.1 If a staff member or Councillor receives an email from another staff member or Councillor which they believe is contrary to the guidance provided in this policy; the staff member or Councillor is entitled to consider use of the Council's grievance policy and/or report the issue through the procedures outlined in the Member's Code of Conduct.

11.1 Compliance and Consequences
Breach of this IT and Email Policy may result in the suspension of IT privileges.

12.1 Policy Review
Updates may be made to address emerging technology trends and security measures
.
13.1 Contacts
For IT-related enquiries or assistance, users can contact the Clerk in the first instance.
All staff and councillors are responsible for the safety and security of Compton Parish Council's IT and email systems. By adhering to this IT and Email Policy, Compton Parish Council aims to create a secure and efficient IT environment that supports its goals.