Approved at the 2nd July 2025 Parish Council Meeting

REVIEWED AND AMENDED MAY 2026 – MIN NO. 26/05/10

TALATON PARISH COUNCIL

EMAIL, INTERNET, AND COMPUTER USE POLICY

Introduction

Talaton Parish Council (`the Council`) provides email facilities for use by Councillors who have access to a desktop, laptops or mobile devices. The Clerk has a designated laptop provided by the Council and has access to email facilities thorough the Council`s E-mail Provider (`the Provider`) and administers the Council's website and Facebook page. This document sets out the Council's policy for the use of these services and more general computer use in compliance with the General Data Protection Regulations.

Objectives

The objectives of this policy are to ensure that the services made available to Councillors and the Clerk are used:

- In accordance with the values, principles, and standards of the Council.
- Ensure GDPR is complied with by ensuring only the Council approved email accounts are used for Council business.
- So as not to incur legal liability.

Acceptance of the Policy

This policy applies to all Councillors & the Clerk. All Councillors and the Clerk are required to sign to indicate their acceptance of the policy content at the time of joining the Council and will be asked to re-affirm their understanding and acceptance of the policy as required.

Each Councillor and the Clerk is individually responsible for complying with this policy.

Security

Access to email accounts and the shared areas through the Provider are restricted to individual users and cannot be shared outside of the Council or between individuals.

Email Accounts:

- The Clerk will be wholly responsible for the Council`s incoming emails, using a specified e-mail address

- When joining the Council, each Councillor will be issued with an email address and will use a dedicated gov.uk email associated with their Council status along with instructions of how to access their mailbox.
- The access of each user is controlled by means of their own password.
- Passwords must be kept confidential and not disclosed to others.
- System generated passwords may be supplied by the Clerk if necessary, but a password re- set must be performed by the Councillor immediately after access is gained.
- Emails should not be forwarded to personal email address; the Council is the Data Controller of all the data it holds and processes, and information should be retained in its own systems.
- Care should be taken not to leave a device that is connected to an email account unlocked or unattended.

File Storage:

The Council stores all its documents on a secure cloud-based system which the Clerk has full access to and Councillors shall have access to through this system.

- Documents should not be shared outside of the Council.
- Guidance on password protection of files is available from the Clerk.
- Care should be taken not to leave a device that is connected unattended or unlocked.
- For further protection of personal data, all files containing names, telephone numbers, addresses and email addresses, etc. must be password protected. These files are likely to take the form of internal databases, registers etc.
- No personal data/confidential documents should be kept on any storage facility e.g. USB's, laptops or personal computers, as this could result in legal action from third parties.

Breaches of security of the computer system e.g., disclosure of personal passwords, giving unauthorised access to emails to external parties, may result in action from the Information Commissioner`s Office (`the ICO`) .

Councillors should notify the Clerk immediately of any suspected data breach or email account hack. The Clerk will then contact the ICO for guidance on the most appropriate way to deal with the breach.

Safeguarding Access to the Council's Systems

To safeguard access to the Council's systems in the event of the Clerk being incapacitated, contact through the Provider will provide access to the Council`s systems, with relevant permissions.

As stated in the email accounts section of this policy, Councillors will use a dedicated.gov.uk email

Email Usage

The Council's email system enables users, to email other members of the Council, the Clerk and individuals outside of the organisation. All users are encouraged to use an email signature, assistance with this can be obtained from the Clerk.

It should not be assumed that any email communication is secure or private. Users should take this into account particularly when emailing confidential or sensitive information. Once an email is sent to an individual outside of the Council, it is beyond the Council's control and is not guaranteed to be confidential.

Hoax and/or suspect emails should be reported to the Clerk. They should not be opened or forwarded but "double deleted" i.e., deleted from the user's "Inbox" and then also from "Deleted Items".

Prohibited Activities:

The following email activities may breach the Councils 'Code of Conduct' and/or prompt action by the ICO:

- Use of Council email accounts for personal purposes.
- Sending or forwarding any material that is obscene, defamatory, or hateful, or which is intended to annoy, harass or intimidate others.
- Sending or forwarding emails which are likely to damage the reputation of the Council.
- Sending or forwarding electronic chain letters.
- Examining, changing, or using another person's files, output or username without explicit authorisation.

TALATON PARISH COUNCIL

To be disseminated yearly at the Annual Meeting of the Council for ongoing acceptance.

I have received, read, understood, and agree to abide by the Council's Email, Internet and Computer Use Policy.

CLERK AND CLLR NAME	CLERK/CLLR SIGNATURE	DATE