

IT and Electronic Communications Policy

UFFORD PARISH COUNCIL

Judi Hallett
CLERK, UFFORD PARISH COUNCIL

Introduction

This IT Policy outlines the principles and guidelines governing the use of IT resources at Ufford Parish Council. The policy aims to safeguard both the confidentiality and integrity of sensitive information, ensure the council's compliance with legal obligations, and provide clear expectations for acceptable use of IT resources.

The Parish Council has a website and uses email to communicate. The Parish Council will always try to use the most effective channel for its communications. Should the Parish Council add to the channels of communication that it uses as it seeks to improve and expand the services it delivers, this policy will be updated to reflect the new arrangements.

This policy applies to any employees, councillors, volunteers, and contractors who have access to the Parish Council's IT systems, networks, and data. It includes the use of all council-owned devices (e.g. laptops, desktop computers, mobile phones), networks, and services such as email, file storage, and website platforms

Communications from the Parish Council – Business Use

Communications from the Parish Council should meet the following criteria:

- Be civil, tasteful and relevant;
- Not contain content that is knowingly unlawful, libelous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive;
- Not contain content knowingly copied from elsewhere, for which the Parish Council does not own the copyright;
- Not contain any personal information, other than necessary basic contact details;
- If official council business, it will be moderated by the Clerk to the Parish Council as the Proper Officer.

Parish Council website

Occasionally, the Parish Council may direct those contacting the Council to its website to see the required information if it is in the public domain. The website can be found at: <https://ufford-suffolk-pc.gov.uk/>

The Parish Council allows and enables approved local groups to have and maintain a presence on its website to present information about the group's activities. The local groups will be responsible for maintaining the content and ensuring that it meets the Parish Council's 'rules and expectations' for the website. The Parish Council reserves the right to remove any or all of a local group's information from the website, if it feels that the content does not meet the Parish Council's 'rules and expectations' for its website.

Parish Council email

The Parish Council has a dedicated email address clerk@ufford-suffolk-uk.gov.uk. The email account is monitored daily and responded to during office hours on Monday to Fridays, and the Parish Council aims to reply to all questions sent as soon as practically possible.

The Clerk is responsible for dealing with emails received and passing on any relevant mail to members or external agencies for information and/or action. All communications on behalf of the Council will come from the Clerk.

Please note that the Clerk works part-time so will respond as soon as they can. The Parish Council may not respond to every comment it receives, particularly if it is experiencing a heavy workload or the comment is for information purposes only.

Emails to the Parish Council become official and will be subject to The Freedom of Information Act 2000 as soon as they are received. Any email sent solely to a Councillor must be forwarded to the Clerk as soon as possible. These procedures will ensure that a complete and proper record of all correspondence is kept.

SMS (Texting and WhatsApp)

Members and the Clerk may use SMS and WhatsApp as a convenient way to communicate at times. All are reminded that this policy also applies to such messages.

Internal communication and access to information within the Parish Council

The Parish Council is continually looking at ways to improve its working and the use of electronic communications is a major factor in delivering improvement. Parish Councillors are expected to abide by the Code of Conduct in all their work on behalf of the Parish Council.

All Parish Councillors have a dedicated email given to them once elected or co-opted onto the Council and should ensure that they do not use any other email addresses when corresponding on council business (e.g. from their personal devices). Council members should access their email via webmail from any browser.

To gain access to Councillors email addresses, members should navigate to <https://webmail.ufford-suffolk-pc.gov.uk> and use their existing username and password which will enable them to log in. Members can easily bookmark this page to enable speedier access.

By using webmail, the council has reduced the danger of a security breach on a member's own device as the emails viewed on webmail are not downloaded to the device used to access them.

As more and more information becomes available electronically, it is vital that all information is treated sensitively and securely. Parish Councillors are expected to maintain an awareness of the confidentiality of information that they have access to and not to share confidential information with anyone. Failure to properly observe confidentiality may be seen as a breach of the Parish Council's Code of Conduct and will be dealt with through its prescribed procedures (at the extreme it may also involve a criminal investigation).

Members should be careful only to cc essential recipients on emails and avoid use of the 'Reply to All' option (whilst ensuring that the people who need to know the information are copied in) and ensure that email trails have been removed.

Incident Reporting

Any IT related incident, such as a suspected data breach, cyberattack, or system failure, should be reported immediately to the Clerk. All incidents will be logged and investigated in line with GDPR's breach notification requirements.

Training

All employees and councillors will undergo IT security training at least once a year.

The training will cover topics such as phishing, data protection, and the correct use of IT resources. New employees and councillors will receive this training as part of their induction process.

General Data Protection Awareness

Whilst parish councils are expected to comply with Data Protection legislation, individual Councillors will also need to ensure that they protect an individual's personal data whether it is stored electronically or as a hard copy. This applies only to living individuals (not the deceased), companies, other authorities and charities. Personal data includes:

- Names and addresses of individuals
- Telephone numbers
- Email addresses
- IP addresses

Compliance & Legal

The council's use of IT resources must comply with all relevant legislation, including the General Data Protection Regulation (GDPR), which governs the processing of personal data. Employees and councillors must be familiar with their responsibilities under this legislation and act in accordance with the data protection principles set out in the GDPR.

Further Guidelines for Councillors

Councillors are requested to implement the following agreed measures to comply with the legislation:

- Only use Ufford Parish Council email account for Parish Council correspondence
- Ensure all Parish Council correspondence includes the Ufford Parish Council footer containing the Privacy Statement or a link to the relevant page on the website (this will be provided by the Clerk)
- Ensure that all devices (computers, laptops, phones) from which council communications are sent are password protected
- Not forward on emails or email threads outside the council as they may contain personal data.
- Delete emails which are no longer required
- As far as possible direct all correspondence to the Clerk, who can, where necessary obtain any required consent
- If holding an individual's information in a Councillor's home or on a Councillor's own PC, the councillor should take particular care to ensure that no one outside the council has access to the file or device in or on which that information is held. Such information needs to be stored securely, for example in a locked room or cabinet (for paper documents) or if on a PC, in a password protected folder or device.
- Ensure that their antivirus software and operating system is up-to-date
- Ensure that their computer's firewall is turned on
- Inform the Clerk of any breaches within 48 hours of discovery

Reviews & Updates

This policy will be reviewed annually or sooner if required by significant changes in legislation or technology. Employees and councillors will be notified of any changes, and they will be required to acknowledge their understanding of the updated policy.

This Policy was adopted by the Council at its meeting held on [17th February 2026](#)

Signed:

D Findley

Chair

J Hallett

Clerk