Email Communications & Acceptable Use Policy

1. Policy Statement

Stapeley & District Parish Council encourages the use of email which supports the aims and objectives of the Council. It is essential that when emailing as a Council member or employee (user) the content complies with current legislation and relevant Council policies and procedures and does not create unnecessary business risk for the Council.

The Council's email facility is made available to users for Council business purposes.

2. Risk Management

The Council recognises that there are risks associated with the use of email and the extensive damage that can be caused by offensive, libellous or defamatory emails.

The Council therefore recognises that there are risks associated with the use of email and the extensive damage that can be caused by:

- Sending or forwarding emails, including an attachment, with any libellous, defamatory, offensive, racist, or obscene remarks.
- Unlawfully forwarding confidential information.
- Unlawfully forwarding or copying messages without permission.
- Sending or forwarding an attachment that contains a virus.

This policy aims to ensure the appropriate access to, and use of the Council's email facility to help mitigate the following risks:

- Harm to individuals
- Damage to the Council's reputation
- Potential legal action and/or fines against the Council or individual(s)
- Inappropriate use of council resources

3. Scope

This policy applies to all employees and members including all elected and co-opted councillors and the Clerk to the Council who have access to the Council's email facility.

Serious breaches of this policy by any Councillor or employee may be dealt with as appropriate. The Council may take disciplinary action. Any breaches of data or data protection may be reported to the Information Commissioner Office (ICO).

4. Email Account

a) All official Council email accounts are hosted on the stapeleyparishcouncil.gov.uk domain.

b) The official email account which represents the council is clerk@stapeleyparishcouncil.gov.uk

c) All members of the council will be issued with an email address which adheres to the format of firstname.lastname@stapeleyparishcouncil.gov.uk Email display names should only appear as Cllr First name Last name.

d) Council email addresses are considered public and can be published on the Council website and within noticeboards.

e) Personal emails and member work emails are not permitted to be used for Council business and all Council email communications should be made via official Council email accounts.

f) Access to email is permitted via webmail. Email clients can be used on devices which are used exclusively by the employee or councillor. If a shared device is being used, then webmail should be used and signed out after each session.

g) Only the employee or Councillor is permitted to view emails sent via official council email.

h) Consideration should be given to if any email should be forwarded outside of the Council as this may share data and information which is privileged information and not intended for a wider audience. Confidential business should not be shared outside of the Council.

i) Access to Council email addresses is permitted during a councillor's term of office or during an employee's tenure of employment. On cessation to ensure that privileged information is not available, email access will be revoked.

j) Council email accounts should be kept ‘tidy’ with good inbox management with received emails deleted and filed as appropriate. Items contained within the sent items should not be deleted.

5. Working Group and Committee Email Addresses

The Council may create dedicated email addresses for use by formally constituted working groups and committees.

These addresses will be general shared mailboxes rather than individual accounts. Access will be granted to all appointed members of the relevant working group or committee so that communications can be managed collectively. This arrangement supports continuity, transparency and efficient handling of correspondence relating to the work of the group.

Where appropriate, these shared addresses may be used as public facing contact points. This allows residents, organisations and stakeholders to communicate directly with the relevant working group or committee and supports the effective delivery of Council business.

All communications sent from or received into these shared mailboxes remain subject to this Email Communications and Acceptable Use Policy and all associated legal and data protection requirements.

All emails sent from a group email address must clearly identify and be signed by the individual author.

6. Email Third Party Instructions

Any official orders or instructions, agreeing to terms, or entering contractual commitments with third parties should come from the Clerk. Councillors would only be permitted to send such emails to third parties with specific prior authorisation from the Clerk.

7. Email Security

a) Email passwords should be kept secure and not shared with other users.

b) All email users should be aware of potential email scams, including phishing attempts. Emails may appear to come from a trusted source but if in doubt of the validity of the email the sender should be confirmed by checking the sending email address and not relying on the sending display name.

c) Any emails received asking for something out of the ordinary or out of character of the sender should be treated with caution and checks completed before any further engagement.

d) Any email received which the user believes is not genuine should be notified to the Clerk.

8. Legal Requirements

The following rules are required by law and are to be strictly adhered to:

a) It is strictly prohibited to send or forward emails containing libellous, defamatory, offensive, racist, or obscene remarks. If an email of this nature is received, promptly notify the Clerk.

b) Do not send unsolicited email messages whereby you would be invading someone's privacy.

c) When sending the same email to multiple external third parties, the email should either be composed as a separate email, or the BCC function should be used. This will ensure that the third-party email addresses are not shared with other recipients.

d) Do not forge or attempt to forge email messages.

e) Do not send email messages using another person's email account.

f) Do not send a copy of a message or attachment belonging to another user without permission of the originator.

g) Do not disguise or attempt to disguise your identity when sending email.

9. Freedom of Information / Right of Access

Email messages may be disclosed under the Data Protection Act 1998, the Freedom of Information Act 2000, or in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered; email messages should be treated as potentially retrievable, either from the main server or using specialist software. Users should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Users should assume that email messages may be read by others and not include anything that would offend or embarrass any reader, or themselves if it found its way into the public domain.

a) In the case of a Freedom of Information / Right of access request made in writing to the clerk pertaining to email communications the clerk will access the relevant Council email accounts to identify the required information. Councillors will be informed of the request prior to information being retrieved.

10. Data Protection

Personal data is subject to the Data Protection Act 2018 which is the UK's implementation of the General Data Protection Regulation (GDPR). Under the terms of the Act, personal data includes any information about a living identifiable individual, including their name, address, phone number, email address and any other information about the individual. If such information is included in an email or an attachment to an email, a user is deemed to be "processing" personal data and must abide by the law. A user must not collect such information without the individual knowing what the user proposes to do with such information. Such information may not be disclosed or amended except in accordance with the purpose for which the information was collected. The user must ensure the information is accurate and up to date. In addition, the individual has the right to inspect what is held about him or her on the email system or held in separate archives of emails. The individual can demand correction of inaccurate information, can request blocking or erasure of damaging information, and can sue for damage caused by inaccurate information.
The law also imposes rules on storing of personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected. If a user maintains their own stores of emails, they should ensure that such stores are not maintained for longer than is necessary for the purpose for which they were collected. Emails should be held in such a way that they can be easily identified, reviewed and when necessary, destroyed.

a) A practical application of the above points would be if an email was received by a member of the public and the content of the email needed to be shared within the Council. Personal information should be redacted, or permission should be confirmed with the sender that personal information can be shared with the content of the communication.

b) Communications from businesses and other formal organisations (as sent from an official email address) are received on the basis of information intended for Council internal sharing and can be forwarded internally as appropriate.

11. Email User's Responsibility

It is each user's responsibility to:

a) Take time to read and understand this policy before using the Council's email facility.
b) Use the Council's email facility strictly in accordance with this policy.
c) Use the Council's email facility responsibly and in a way that will not harm the Council's reputation.
d) Take care to ensure that emails are sent only to those who should receive them. Re-read emails before sending, check for correct addressing (particularly where they include personal or sensitive information), and clarity, and to ensure that the content will not embarrass or subject the Council to legal proceedings or a fine.
e) Send messages containing statements which are likely to create liability (whether criminal or civil, and whether for you or the Council).
f) Ensure that personal opinion is not represented as that of the Council.
g) Send commercial or advertising material, chain letters, or junk mail (otherwise known as spam) of any kind.
h) Not subscribe to mailing lists for personal purposes using your Council email address.
i) Recognise that the Council's email facility is provided for Council use and that it is to be used within the scope of being an elected or co-opted Councillor or an employee of the Council.
j) Report any misuse of the Council's email facility.
k) Ensure that the use of email is consistent with the Council's Code of Conduct.

This policy was adopted by Council at the meeting held on the 16th February 2026.