Chandler's Ford Parish Council

IT and Email Policy

Purpose

Chandler's Ford Parish Council's (CFPC) internet facility exists to support the organisation's business requirements. Appropriate use of the internet and email facility is acceptable, provided that the conditions specified in this policy are met, including requirements relating to security, confidentiality and compliance with relevant legislation.

With the ever-increasing use and variety of social media consideration must be given to the appropriate use by staff and Councillors to ensure that it is effective, lawful and does not compromise Council information or computer systems / networks.

Equipment

IT equipment, hardware and software are the property of CFPC. Authorised users are responsible for its security and appropriate use.

Staff must not attempt to modify or alter the hardware without the authorisation of the Clerk. Similarly, no attempt should be made to modify, delete or alter the set-up of the windows environment or any software loaded on council workstations. Any new software should only be installed by the Council's IT contractor with the authority of the Clerk.

The making of illegal copies of software, or any other action that could violate software licence agreements are prohibited.

Faults

In the event of any hardware or software fault authorised users are required to contact the Clerk or, if not available, the council's appointed IT contractor.

Acceptable Use of the Internet

No use of the internet is permitted without the active use of a firewall and up-to-date anti-virus.

It is prohibited to intentionally use internet resources to access, transmit or retrieve any material or communications that are –

- obscene
- sexually explicit
- discriminatory or harassing nature
- derogatory to any individual or group
- threatening in nature

Software or files that are not connected with your work for Chandler's Ford Parish Council should not be download.

Any sites which require registration or payment for services must not be accessed without the authority of the Clerk.

Use of Email

The use of email to exchange correspondence requires the same professional standards as other forms of communication. You should not send or forward mail which is defamatory or offensive for whatever reason.

In order to protect the Council's equipment and data from viruses, email attachments which might contain macros (word processor and spreadsheet files) or applications, should not be opened if they are from an unknown sender. They should be deleted.

When constructing an email the following points should be observed –

- A subject of the email within the subject line should be well defined.
- Use "Urgent" appropriately.
- Use appropriate formality at the start and finish of any email.
- Check grammar and spelling.
- Emails should not commit the Parish Council in any way without prior authorisation of the Clerk.
- Use block capitals or bold text appropriately as this can be interpreted as aggressive.
- Use the confidential disclaimer when email contents are sensitive and not to be shared or forwarded.

Staff should be aware that emails received or sent may be retained in an overall system archive, even if they have been deleted from your own email account. This is to ensure that CFPC complies with Data Protection Laws and in accordance policy.

Staff must also ensure that the suitable signature footer is used as standard which states confidential nature of email along with compliance to the Freedom of Information Act 2000 or other legal duty.

CFPC acknowledges the Information Commissioners Office Guidance on the use of emails and personal emails and has opted to exceed the standards suggested by adopting an allocated specific email address using the parish domain for councillors and staff in accordance with HALC recommendation.

Councillors should only use email accounts provided by CFPC for Parish Council business and not private or personal email accounts. Any email account may be subject to full investigation by the Information Commissioner's Office as part of a GDPR breach.

Please be aware when adding personal comments or forwarding email chains without first checking that the content is suitable for the recipient.

Be vigilant for phishing emails attempting to obtain personal information or credentials. If in doubt do not click on links and report any suspicious messages to the Clerk.

Emails should be retained in accordance with the Council's Records Retention Policy.

Data protection

To comply with the Data Protection Act 2018 personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Care should be taken that private email addresses are not inadvertently circulated. Private email addresses should be treated as confidential. Emails to multiple addresses outside of Councillors and the Clerk, should be sent as a blind carbon copy (bcc).

All staff and Councillors are required to report any suspected data breach or loss of personal data immediately to the Clerk, who will investigate. Passwords for all systems must be kept confidential, changed regularly, and comply with good security practice. Sensitive personal data should be transmitted only via encrypted email or secure methods approved by the Clerk.

The principles of this policy apply to any communication or publication on social media where you are acting in your capacity as a representative of CFPC. For more information regarding social media, please refer to the Communications and Media Policy.

Failure to comply with this policy may result in disciplinary action.

This policy will be reviewed every two years. All new members and employees will be provided with a copy of this policy.

Policy version – IT&E2025
Resolved by Policy and Finance Committee – 15 September 2025
Adopted by Full Council – 29 September 2025
Date for next review – September 2027