Cranleigh Parish Council

# EMAIL AND INTERNET USAGE POLICY

## 1. Introduction

1.1 The Council recognises that email and internet are important information and communication systems which are used during the course of council business. This policy provides guidelines and procedures to protect users and the council.

1.2 This policy applies to all staff members who have access to the internet and email facilities via council computers.

1.3 The email policy applies to all councillors in their correspondence with staff members and/or other councillors.

## 2. Internet usage

2.1 Staff members are encouraged to use the internet responsibly as part of their official and professional activities.

2.2 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.

2.3 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.

2.4 The use of the internet to access and/or distribute any kind of offensive material will not be tolerated and staff may be subject to disciplinary action.

2.5 The equipment, services and technology used to access the internet must only be those authorised for this purpose by the council, or the property of the council. The council reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

## 3. Unacceptable use of the internet

3.1 Unacceptable use of the internet by staff members includes, but is not limited to:

- sending or posting discriminatory, harassing or threatening messages or images
- using computers to perpetrate any form of fraud, and/or software, film or music piracy
- obtaining, using or disclosing another staff member's password without authorisation
- sharing confidential material or proprietary information outside of the council
- hacking into unauthorised websites
- sending or posting information that is defamatory to the council, its services, councillors and/or members of the public
- introducing malicious software onto council computers and/or jeopardising the security of the council's electronic communication systems
- sending or posting chain letters, solicitations or advertisements not related to Council business or activities
- passing off personal views as those representing the Council
- accessing inappropriate internet sites, web pages or chat rooms
- Creating accounts on Social Media or other services on behalf of the council without the authorisation of the Council or responsible officer.

3.2 If a staff member is unsure about what constitutes acceptable internet usage, then he/she should ask his/her line manager for further guidance and clarification

## 4. Email

4.1 Use of email is encouraged as it provides an efficient system of communication.

4.2 Email should be regarded as written paper documents for the purposes of production, use, retention and disclosure and can be called upon under the Freedom of Information Act 2000. Personal information should be kept in accordance with the principles established in the Data Protection Act 1998.

4.3 The Council reserves the right to open any email file stored on the Council's computer system.

4.4 The following guidelines for email use should be observed by all staff members and councillors:

- use appropriate language to avoid unintentional misunderstandings
- respect the confidentiality of information contained within emails, even if encountered inadvertently

- Quarantine any email received if there is any doubt regarding the authenticity of a message and verify the authenticity of the sender, without risk to the council by contacting them directly.
- do not open any attachment unless certain of the authenticity of the sender
- only copy emails to others where appropriate, certain of the authenticity of the sender and necessary
- emails which create obligations or give instructions on behalf of the council must be sent by officers only, not councillors
- emails must comply with common codes of courtesy, decency and privacy

## 5. Reporting and sanctions

5.1 If a Councillor receives an email from a staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the Council's formal disciplinary procedure, or refer the matter to the Personnel Committee depending on the severity of the event.

5.2 If a staff member receives an email from another staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the Council's formal disciplinary procedure, or refer the matter to the Personnel Committee depending on the severity of the event.

5.3 If a staff member receives an email from a Councillor which they believe is contrary to the guidance provided in this policy, the staff member 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.

## 6. Security

6.1 Only software purchased by the council shall be installed on the Council's computer system. Software licences shall be retained.

6.2 If a council officer's or councillor's computer is compromised by malicious, or foreign sovereign insurgency, the officer or councillor must immediately contact the councils IT and IT security team and disconnect their device from any threat to the councils network and systems.

6.3 Any breach of security perceived by any councillor or officer of the Council's IT systems by virtue of incursion by malicious software, or third parties must be reported to the Responsible Officer and the council's IT and network support provider: Netcom It Solutions Limited 01403 252995.

October 2022

**Policy Review Date: October 2026**