ELLISFIELD PARISH COUNCIL

IT AND EMAIL POLICY

1. Introduction

Ellisfield Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations and communications.

This policy provides guidelines, responsibilities and procedures for the appropriate use of IT resources and email to protect users and the Council.

This policy should be read in conjunction with the Council's Data Protection Policy and Data Retention Policy .

All users of the Council's IT, email and internet facilities need to be aware that under the Data Protection and Freedom of Information Acts, internet and email usage reports and documents on Council computers may have to be disclosed when the Council responds to a Freedom of Information or Subject Access Request.

2. Scope

This policy applies to all staff members, councillors, contractors and volunteers who have access to the Council's IT resources, including computers, networks, software, devices, data, or council-owned email accounts.

The Council endeavours to provide required devices to staff but acknowledges that members and any others with council-owned email accounts will be using their own personal devices such as private computers, phones or tablets and staff may use some personal devices . Everyone must adhere to this policy to maintain digital security.

3. Training and awareness

The Council will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. They should engage in regular training on email security and best practices, including but not limited to:

- the Parish Council Domain Helper Service's virtual cybersecurity workshops for councils

- The National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

4. Acceptable use of council-provided IT resources and email

When using council-provided IT resources and email accounts for the council's purposes, users must adhere to ethical standards, and respect copyright and intellectual property rights. Council-provided email accounts are to be used for official council-related activities and tasks. Limited personal use of IT resources is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

Where possible, authorised devices, software, and applications will be provided by the Council for work-related tasks. Users must not install unauthorised software without permission.

Users must not use council equipment or council email accounts to access or forward inappropriate or offensive content.

5. What you must do if you use your own personal devices

If using your own device for council business, users must make sure they are:

- using strong passwords for all their accounts (preferably using a password manager)
- downloading the latest operating system security updates
- using anti-virus software

6. Mobile devices and remote working

Mobile devices provided by Ellisfield Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

7. Network and Internet usage

All users using the internet for work tasks must use the internet responsibly as part of their official and professional activities. Information obtained via the internet and published in the name of the Council must be relevant and professional.

Users must be careful about which Wi-Fi networks they join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. They should always make sure they are using a trusted internet connection, which is password protected when carrying out official business.

Unacceptable use of the internet by users 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 room

8. Email Communication

Only Council-owned email accounts must be used to conduct Council business. Personal email accounts must not be used for Council business due to potential data breaches, issues

surrounding Freedom of Information or Subject Access Requests and general recommended good practice for local councils.

Emails must not be auto-forwarded to any other account. This may result in confidential information being disclosed to unauthorised people.

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 General Data Protection Regulations and other relevant legislation.

All Council email accounts have a private password that should be kept confidential by the user/s of that account and not shared. The Council has administrative control over email accounts and can reset passwords and give access to email accounts, where needed.

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

Care needs to be taken when registering Council email addresses on websites such as discussion forums, news groups, mailing lists, blogs etc to prevent email address being used for other purposes.

Whilst emails are generally open and transparent, some emails may not be received or read, and they may be intercepted or disclosed by other people. Users must decide whether email is the best way to exchange confidential or sensitive information.

Care must be taken when addressing emails, particularly those including sensitive, confidential or restricted information, to avoid accidentally sending them to the wrong people. Particular care must be taken with auto-completion of an email address.

All Council business emails and documents sent by users are the property of the Council and not of any individual user.

Council email address (or indeed internet or computer facilities) must not be used for:

- commercial or personal profit-making purposes or other form of financial gain (e.g. in connection with any employment other than that associated with the Council);
- activities that lead to unauthorised expenditure for the Council (e.g. excessive printing or photocopying that is not Council business);
- activities that go against Council policies or standards;
- personal interest group activity outside of a user's role;
- activities that may cause damage, disruption, fines, penalties or negative media attention for the Council;
- excessive email conversations that may be interpreted as misuse.

The following guidelines for email use should be observed by all users of town council email addresses:

- think before copying someone into an email conversation.
- avoid replying to all unless absolutely necessary.
- use appropriate language to avoid unintentional misunderstandings
- respect the confidentiality of information contained within emails, even if encountered inadvertently

- check with the sender if there is any doubt regarding the authenticity of a message
- do not open any attachment or open any links in emails unless certain of the authenticity of the sender, in order to avoid malware or phishing.
- emails which create obligations or give instructions on behalf of the Council must be sent by officers only, not councillors or other individuals
- emails must comply with common codes of courtesy, decency and privacy
- emails should be professional and respectful in tone.

9. Email Access

The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. The Clerk may need to access councillors's emails so that they can respond to FOI or subject-access requests. A personal email accounts should not be used for council business, but if for any reason it were, it is still subject to data protections laws and FOI requests.

10. Password and Account Security

Users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. The National Cyber Security Centre's advice for choosing a strong password gives guidance on passwords. Regular password changes are encouraged to enhance security.

For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

11. Data Management, Data Retention and Security

All sensitive and confidential data should be stored and transmitted securely. Users must regularly backup any important data to prevent data loss and the Council's Data Retention Policy.

Users should retain and archive emails in compliance with the Data Retention Policy. They should regularly review and delete unnecessary emails to maintain an organised inbox

12. Reporting security incidents

All suspected security breaches, including email breaches or incidents should be reported immediately to the Clerk for investigation and resolution.

13. Compliance and consequences

Any breaches in this IT and Email Policy will be investigated and any action arising will follow the council's disciplinary procedures.

14. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.