Horsmonden Parish Council IT Policy

1. Introduction

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

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use Horsmonden Parish Council's IT resources, including computers, networks, software, devices, data (including CCTV footage), and email accounts.

3. Acceptable use of IT resources and email

Horsmonden Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Horsmonden Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5.Use of own devices

Clerks and Councillors are provided with laptops, and Clerks are provided with work telephones . Bearing this in mind emails should not be accessed using personal devices. Councillors may communicate via WhatsApp/text messaging on own devices to alert one another/or the Clerks about non specifics or to ask others to read emails sent on the council laptops.

6. Data management and security

All sensitive and confidential Horsmonden Parish Council data (including CCTV footage) is stored and transmitted securely using approved methods. CCTV footage is secured on a protected network and remote access to footage is encrypted with password protection and authentication applied. Footage is only accessed by authorised personal when required for an incident, investigation of lawful request . It may in these instances be shared with law enforcement agencies. CCTV footage is automatically overwritten after 30 days if not required for ongoing investigation .

All other data is regularly backed up and stored within the UK by a contracted IT company, to prevent data loss or breach . The storage of data is reviewed regularly and secure data destruction methods are used when necessary.

7. Network and internet usage

Horsmonden Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

8. Email communication

Email accounts provided by Horsmonden Parish Council are for official communication only. Emails should be professional and respectful in tone.

Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

9. Use of Social Media

All use of social media shall be in accordance with Horsmonden Parish Councils Social media policy whatever device it is accessed on .

10.Password and account security

Horsmonden Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

11. Mobile devices and remote Work

Mobile devices provided by Horsmonden 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.

12. Email monitoring

Horsmonden Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

13. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements as well as Horsmonden PCs retention policy . CCTV footage is automatically overwritten after 30 day if not required for ongoing investigation

14. Reporting security incidents

All suspected security breaches or incidents, whether relating to email security or other data security, should be reported immediately to the Clerk and/or the Data Protection Officer for investigation and resolution.

15. Training and awareness

Horsmonden Parish Council offers regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

16. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

17. 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.

18. Contacts

For IT-related enquiries or assistance, users can contact Arron services for hardware related issues or Microshade VSM for software issues .

All staff and councillors are responsible for the safety and security of Horsmonden Parish Council's IT and email systems. By adhering to this IT and Email Policy, Horsmonden Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.