EWHURST PARISH COUNCIL WITH ELLENS GREEN

IT and Email Policy

1. **Introduction**
   Ewhurst Parish Council recognises the importance of effective and secure information technology (IT) and email use 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 Ewhurst Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.
   [1. It also applies when council email or data is accessed on personal devices, such as laptops, tablets, or smartphones.]

---

3. **Acceptable use of IT resources and email**
   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, is lawful, and does not breach this policy.
   [2. All official council business must be conducted using the council-issued email address; personal email accounts must not be used for council communications.]
   All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

---

4. **Device and software use**
   Where possible, authorised devices, software, and applications will be provided by the Council for work-related purposes.
   [3. When using personal devices for council business, users must ensure devices are password/PIN protected, have current security updates, and, where possible, encryption enabled.]
   Unauthorised installation of software or use of unapproved devices is prohibited.

---

5. **Data management and security**
   All sensitive and confidential council data must be stored and transmitted securely using approved methods.
   [4. Any loss, theft, or compromise of a device containing council data must be reported immediately to the Clerk.]

---

6. **Network and internet usage**
   Council internet connections should be used responsibly and efficiently for official purposes. Downloading or sharing copyrighted material without permission is prohibited.

7. **Email communication**
   Council-provided email accounts are for official correspondence only.
   Emails must be professional, factual, and respectful.
   Exercise caution with attachments and links to avoid phishing and malware.

---

8. **Password and account security**
   Users are responsible for maintaining the security of their accounts and passwords.
   Passwords must be strong, unique, and not shared.
   Regular password changes are encouraged.

---

9. **Mobile devices and remote work**
   [5. All devices used to access council data must have screen-lock enabled, antivirus protection (where applicable), and remote wipe capability if possible.]
   When working remotely, ensure no one else can access council information.

---

10. **Email monitoring**
    The Council reserves the right to monitor email communications for compliance with this policy and legal requirements, in accordance with data protection law.

---

11. **Retention and archiving**
    Emails should be retained and deleted in accordance with legal and regulatory requirements.
    [6. Councillors should avoid storing council data indefinitely on personal devices and use council systems for archiving where available.]

---

12. **Reporting security incidents**
    All suspected security breaches must be reported immediately to the Clerk at clerk@ewhurstellensgreen-pc.gov.uk

Notes:

1. *Personal devices clause* – ensures security when councillors access email on their own phones or laptops.
2. *Council email only* – keeps records centralised and protects against data loss or FOI problems.
3. *Screen lock / password rules* – prevents unauthorised access if a device is lost.
4. *Immediate breach reporting* – meets GDPR's 72-hour rule for notifying the ICO.
5. *Screen-lock / antivirus / remote-wipe rule* – strengthens security for any device used to access council data, reducing the risk of loss or unauthorised access.
6. *Monitoring and retention wording* – ensures compliance with data protection law.