Artington Parish Council

Information Technology and Acceptable Use Policy

---

1. Purpose

This Policy defines the standards of acceptable use of information technology (IT) resources, including computer equipment, networks, email and internet, by councillors, staff, volunteers, contractors and others (collectively "Users") of the Artington Parish Council ("the Council"). It aims to protect the Council's IT assets, data (especially personal or sensitive data), and to ensure compliance with legal obligations (including the UK Data Protection Act 2018, the General Data Protection Regulation (UK GDPR) and the Transparency Code for Smaller Authorities).

2. Scope

This Policy applies to:

- All IT hardware, software, networks, email accounts, cloud services and data owned, leased or used by the Council.
- All users of the Council's IT resources: councillors, clerk, employees, volunteers, contractors or others acting on its behalf.
- Use of personal devices (BYOD) or personal email accounts when used for Council business.
- All data processed, stored or transmitted in the course of Council business.

3. Roles and Responsibilities

- **Council**: Ensure appropriate IT policy, oversight, budgeting, training and review.
- **Clerk / Responsible Officer**: Day-to-day management of the Council's IT resources, ensure backups, ensure users are aware of policy, monitor compliance.
- **Users**: Comply with this Policy, report any security incident or suspected breach immediately, use IT resources responsibly.

4. Acceptable Use

4.1 General

- IT resources are provided primarily for official Council business.
- Limited personal use may be permitted (at the Council's discretion) provided it does not interfere with official duties, compromise security or violate other policies.
- Use must be lawful, ethical and respectful of others; no accessing or storing of inappropriate, offensive, illegal or unlicensed content.
- Copyright and intellectual property rights must be respected.

4.2 Email / Communications

- Councillors, the clerk and staff should use official Council-managed email accounts for Council business; personal email accounts should *not* be used for sending or receiving substantive Council business.
- Email signatures and disclaimers may be used as agreed by the Council.
- Caution must be exercised with attachments, links and un-trusted senders; phishing and malware are significant risks.
- Confidential or sensitive information must only be sent by approved secure methods (e.g., encrypted attachments or secure portals) and in line with the Council's Data Protection / Privacy Policy.

4.3 Internet / Network Use

- Internet access must be used in line with this Policy. Downloading or sharing of copyrighted material (e.g., films, music, software) without proper authorisation is prohibited.
- The use of social media for official Council business must be in line with the Council's Social Media policy (if any) and only authorised users should post/ engage.

5. Device, Software and Data Management

- All hardware, software, devices and licences must be recorded on the Council's asset register (where applicable).
- Devices provided by the Council remain property of the Council. On termination of office/employment/contract the device must be returned and Council data removed/securely destroyed.
- Personal devices (BYOD) using Council systems must be approved and subject to security safeguards (passwords, encryption, updates etc).
- Software must be kept up to date (patching) and only authorised software may be used.
- All digital documents and data must be stored appropriately (e.g., on the designated Council drive or cloud storage as approved); storing Council business on personal/local drives or devices is discouraged or must follow approved processes.
- Adequate backup arrangements must be maintained and data recovery plans considered.
- When data or devices are retired or disposed of, data must be securely destroyed.

6. Security and Passwords

- Users must use strong passwords and must not share passwords or accounts.
- Where available, two-factor authentication (2FA) should be used.
- Users must lock or log-off devices when unattended and ensure devices are secured.
- No unauthorised access to data, programs or networks.
- If a device is lost, stolen or compromised, it must be reported immediately to the clerk/chair.
- Regular security awareness training or guidance should be provided.

7. Remote Working / Mobile Devices

- When working remotely or using mobile devices, users must adhere to the same security standards as in the office.
- Ensure secure VPN/remote access if required; use encryption if sensitive data is accessed.
- Council devices must be secured with passcodes, biometrics or other approved security methods.

8. Data Protection / Privacy / Personal Data

- Users must comply with UK GDPR and the Data Protection Act 2018 when processing personal or special category data.
- Personal data must not be stored or transferred insecurely; any breach or loss must be reported promptly.
- Use of personal email accounts, cloud services or third-party services must be authorised by the Council when used for Council business and must meet security standards.

9. Website / Accessibility / Communications

- The Council's website must meet accessibility standards (e.g., WCAG 2.2 AA) and be reviewed regularly.
- All official communications posted on social media or website must be consistent with the Council's communication policy, and only authorised persons may post.
- Autoresponders, forwarding of Council email to personal accounts and private email usage for Council business should be avoided.

10. Monitoring and Audit

- The Council reserves the right to monitor the use of its IT resources, within legal limits, to ensure compliance and investigate misuse.
- Users should have no expectation of privacy in terms of content stored or transmitted on Council systems (other than rights under applicable laws).
- An annual (or more frequent) risk assessment should be carried out of the Council's IT systems, data threats and usage.

11. Misuse and Sanctions

- Misuse of IT resources may result in disciplinary action, revocation of access, or other action as determined by the Council.
- Incidents of non-compliance, security breaches or data losses must be reported immediately and will be investigated.

12. Training and Review

- All users must receive appropriate induction/training on this Policy, particularly councillors and staff handling sensitive data.
- This Policy shall be reviewed at least annually (or sooner if required by changes in technology, law or Council circumstances).

13. Approval and Adoption

This Policy was approved and adopted by the Council at its meeting on 12 January 2026.

Next review date: Jan 2027.