Tunbridge Wells Commons Conservators:

Information Technology (IT)Policy

1. Introduction

Tunbridge Wells Commons Conservators (the Conservators) recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications. The purpose of this policy is to ensure that all IT equipment and software, whether owned by the authority or used by staff, members, or other authorised persons (including personal devices when used for authority business), are used in a manner which is secure, legal, and consistent with our obligations under the GDPR 2016, Data Protection Act 2018, Freedom of Information Act, the Transparency Code, and the new digital/data compliance requirements in the Practitioners' Guide (Assertion 10).

2. Scope

This policy applies to:

- The Conservators, officers, volunteers, contractors, or anyone else who uses IT equipment, software, or services in connection with the authority.
- All IT systems, devices, software, applications and communications whether owned by TWCC or personal (when used for authority business).
- All data handled in the course of business activities (including storage, transmission, backups, sharing, deletion).

3. Acceptable use of IT resources and email

The Conservators' IT resources and email accounts are to be used for official business-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights, and must not access inappropriate or offensive content.

4. Device and software usage

The Conservators can provide IT equipment to Officers for work-related tasks. The equipment should be configured with appropriate security (antivirus, firewall, latest updates/patches), should only have authorised software/applications installed on them and the devices should be physically secured when not in use.

Conservators use their own personal equipment in their roles, unless agreed otherwise. Their equipment should be configured with appropriate security and used appropriately to ensure that data protection is not compromised.

5. Data management and security

All sensitive and confidential data should be stored on the OneDrive and transmitted securely. Downloading and sharing authority related material without proper authorisation is prohibited.

Regular data backups should be performed to prevent data loss. Any files or folders containing personal data should be reviewed annually and, where necessary, deleted in accordance with the GDPR policy.

6. Email communication

Email accounts provided by the Conservators 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.

The Conservators reserve 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.

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox. Any emails containing personal data should be reviewed annually and, where necessary, deleted in accordance with the GDPR policy.

7. Password and account security

All 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.

8. Reporting security incidents

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

9. Training and awareness

Where requested, the Conservators will provide resources to educate users about IT security best practices, privacy concerns, and technology updates.

10. Monitoring and review

This policy will also be reviewed following any significant changes: legal/regulation changes, breach/incidents, significant changes in how IT is used by the authority. The authority will document evidence of compliance to support AGAR / external audit purposes.

11. Policy enforcement

Violations of this policy may result in disciplinary action for Officers, or other remedial action for Conservators/others. Undertaking Conservator business using IT in a way that breaches laws and or regulations may have legal consequences.

Date of review: October 2026

Date of next review: October 2027