Godalming
Town Council
Supporting Our Community

IT, CYBER SECURITY & ACCEPTABLE USE POLICY

This policy should be read in conjunction with the linked policies listed below:

- Code of Conduct
- Disciplinary Procedure & Rules
- Equality & Diversity Policy
- Data Protection Policy
- Social Media Policy

1. PURPOSE

The purpose of this policy is to ensure that the Council's information, systems and digital services are used securely, lawfully and sensibly, while supporting efficient day-to-day working.

The Council uses both remote server and cloud-based systems to store and manage information. These systems are critical to service delivery and must be protected from loss, misuse and unauthorised access.

2. SCOPE

This policy applies to:

- all employees, councillors, volunteers and contractors;
- anyone using Council information, systems or equipment; and
- all locations, including remote and home working.

It applies regardless of whether Council systems are accessed using Council-owned or approved personal devices.

3. SYSTEMS COVERED BY THIS POLICY

This policy covers all Council digital systems, including but not limited to:

- Microsoft 365 (Outlook, SharePoint, OneDrive, Teams);
- any remote or hosted servers used by the Council;
- email, internet access and cloud services;
- Council-owned computers, laptops, tablets and mobile phones; and
- approved personal devices used to access Council systems.

4. ROLES AND RESPONSIBILITIES

4.1 The Council

The Council owns all data created, received or stored in connection with Council business.

4.2 Chief Executive Officer

The CEO has overall responsibility for:

- information security and acceptable use;
- ensuring this policy is implemented and reviewed; and
- liaison with the Council's external IT support provider.

4.3 External IT support provider
The Council's appointed IT provider is responsible for:

- technical management of systems;
- security monitoring and updates; and
- supporting incident response and recovery.

4.4 Users
All users are responsible for:

- using Council systems appropriately;
- protecting access credentials and devices; and
- reporting security concerns or incidents immediately.

5. ACCEPTABLE USE

Council IT systems are provided primarily for Council business. Limited personal use is permitted provided that it:

- is reasonable and occasional;
- does not interfere with work;
- is lawful and appropriate; and
- does not risk the security or reputation of the Council.

All use of Council systems must comply with this policy and the Council's other policies, including the Code of Conduct and Data Protection Policy.

Users must not misuse IT facilities in any way that brings the Council into disrepute, causes offence, disrupts operations or jeopardises security.

6. MICROSOFT 365, SHAREPOINT AND RECORDS

As the Council transitions to SharePoint it will become the Council's primary document and records store.

- Council documents must not be stored permanently on local drives or personal devices.
- OneDrive may be used for working files but is not a long-term records store.
- Teams messages and files relating to Council business are Council records.
- Access to files is controlled by permissions, not by copying or downloading unnecessarily.

Users must not create unofficial systems or workarounds that bypass these controls.

7. DATA MANAGEMENT, BACKUPS AND SECURE DISPOSAL

All sensitive or confidential Council information must be stored and transmitted securely using approved systems and methods.

The Council's systems are backed up regularly through approved arrangements with its IT provider.

Where information is no longer required, secure disposal or deletion methods must be followed in line with the Council's Retention and Data Protection Policies.

8. EMAIL COMMUNICATIONS

Council email accounts are for official communication and must be used professionally and respectfully.

Users must:
- avoid sending sensitive or confidential information by email unless it is encrypted;
- exercise caution with attachments and links to prevent phishing or malware;
- verify unusual requests for payment, passwords or information before responding.

Emails should be treated as permanent records and may be subject to disclosure under GDPR or Freedom of Information legislation.

9. SECURITY AND ACCESS

- Each user must have a unique account.
- Passwords must not be shared.
- Multi-factor authentication must be used where available.
- Devices must be locked when unattended.
- Software may only be installed or approved by the Council's IT provider.

Deliberate unauthorised access to systems or data may be a criminal offence.

10. REMOTE WORKING AND PERSONAL DEVICES

Remote access is permitted where approved by the Council.

Where personal devices are used:
- devices must be password protected;
- automatic locking must be enabled;
- Council data must only be accessed via approved applications; and
- Council data must not be stored locally unless authorised.

Lost, stolen or compromised devices must be reported immediately.

11. NETWORK AND INTERNET USE

Council internet access must be used responsibly for official purposes.

Users must not:
- download unauthorised or copyrighted material;
- attempt to bypass security controls;
- introduce malware or unapproved software.

12. MONITORING AND PRIVACY

Council IT systems are monitored to:

- maintain security;
- ensure compliance with policies; and
- support business continuity.

Users should have no expectation of privacy when using Council systems. Monitoring will be lawful, proportionate and for legitimate purposes only.

13. RETENTION AND ARCHIVING

Council emails and electronic records must be retained and archived in accordance with:
- the Council's Retention Policy;
- GDPR requirements; and
- Freedom of Information obligations.

Users should not keep unnecessary emails or duplicate records.

14. INCIDENT REPORTING

All users must report any actual or suspected security incidents without delay, including:

- lost or stolen devices;
- suspected phishing or suspicious emails;
- accidental disclosure of information; and
- unauthorised access to systems.

Incidents should be reported to the Chief Executive Officer, who will coordinate action with the IT provider and follow data breach procedures where required.

15. TRAINING AND AWARENESS

The Council will provide periodic training and guidance to employees and councillors on:
- cyber security best practice;
- phishing awareness;
- safe use of Council systems; and
- data protection responsibilities.

All users are expected to engage with training provided.

16. MISUSE, BREACHES AND ENFORCEMENT

Misuse includes, but is not limited to:

- accessing or distributing illegal or offensive material;
- circumventing security controls;
- introducing malware or unauthorised software;
- excessive personal use; and
- using systems in a way that brings the Council into disrepute.

Failure to comply with this policy may result in:
- withdrawal of system access;
- disciplinary action; and
- referral to external authorities where required.

17. CONTACTS

For IT-related enquiries, assistance or incident reporting, users should contact:
- the Chief Executive Officer; or
- the Council's appointed external IT support provider.

13. REVIEW

This policy will be reviewed annually, or sooner if required by changes in technology, legislation or working practices.