QUEDGELEY TOWN COUNCIL
"Working with the community for the community"

LOCAL COUNCIL AWARD SCHEME QUALITY GOLD

01452 721 552
Quedgeley.gov.uk

Quedgeley Town Council

Information Technology Policy

Policy owner: Jacquie Webster
Approved by: Full Council
Date approved:
Review date: 01/04/2027
Version: Draft 1.0

Policy statement

The Council uses information technology to provide public services, communicate with residents, manage records, help with decision-making, and meet its legal duties.

This policy explains how to use Council IT safely, legally, and effectively. It covers systems, accounts, devices, networks, software, data, and digital services. It should be used together with the Council's other policies, such as Data Protection, Data Retention, Social Media, Freedom of Information, Member and Staff Conduct, Health and Safety, Business Continuity, and other Council procedures.

The Council will manage IT and cybersecurity based on risk and what is reasonable for its size. It will follow official UK guidance, including advice from the National Cyber Security Centre, the Information Commissioner's Office, and other government frameworks.

---

1. Purpose

The purpose of this policy is to:

- Set clear expectations for councillors, employees, contractors, volunteers and other authorised users.
- Protect Council data, systems, devices, accounts and digital services from accidental loss, misuse, unauthorised access, cyber-attack, physical damage and avoidable disruption.
- Support compliance with UK GDPR, the Data Protection Act 2018, Freedom of Information obligations, records management duties and other relevant legal requirements.
- Ensure Council IT resources are used responsibly, securely, lawfully and primarily for Council business.
- Provide clear reporting routes for IT incidents, cyber incidents, data breaches and suspected misuse.
- Support continuity of Council operations in the event of cyber-attack, system failure, fire, flood, electrical damage or other major disruption.

4. Guiding principles

The Council will apply the following principles:

- Security by default: systems, accounts and devices should be configured securely before being used for Council business.
- Least privilege: users should only have access to the systems (computer programs or digital services) and information they need for their role, and no more.
- Accountability: all users are responsible for using IT safely and reporting concerns promptly.
- Proportionality: security controls should be proportionate to the Council's size, resources, legal duties, data sensitivity and operational risks.
- Resilience: the Council should be able to continue essential functions and recover key data following an incident.
- Lawfulness and transparency: monitoring, data handling and record keeping must be lawful, fair, necessary and proportionate.
- Separation of Council and personal activity: Council information, accounts and devices must be kept separate from personal, party-political, commercial or unrelated activity wherever possible.
- Continuous improvement: cyber risk, technology and threats change over time, so this policy and related procedures must be reviewed regularly.

5. Roles and responsibilities

5.1 Full Council or delegated committee

The Council is responsible for:

- approving this policy and any significant changes;
- ensuring IT and cyber risks are considered as part of governance, audit and risk management;
- ensuring proportionate resources are available to manage IT and cyber security;
- receiving reports on major IT incidents, cyber incidents, data breaches and business continuity failures;
- ensuring learning from incidents is acted upon.

5.2 Clerk / Proper Officer / Responsible Officer

The Clerk / Proper Officer is responsible for:

- day-to-day implementation of this policy;
- ensuring users are made aware of their responsibilities;
- maintaining or arranging an inventory of Council IT assets, accounts and key systems;
- ensuring new users, leavers and role changes are managed appropriately;
- liaising with the IT provider, Data Protection Officer, insurer, police, regulators or legal adviser where required;
- coordinating incident reporting and escalation;
- arranging periodic review of this policy.

5.3 Responsible Financial Officer

The Responsible Financial Officer is responsible for ensuring that finance systems, payment systems, banking access, accounting records and financial data are subject to suitable controls, including access restrictions, segregation of duties, secure authentication and backup arrangements.

5.4 IT provider or system administrator

If the Council uses an external IT provider or system administrator, they are responsible within their contract or agreed role. Their duties are: configuring systems and devices securely; applying updates and patches; managing antivirus, endpoint protection, firewalls, and other technical controls; maintaining backups and restoration if contracted; supporting access control and account management; advising on cyber risk and improvements; and supporting incident response and recovery.
The Council should ensure that contracts or agreements clearly define responsibilities. These cover backup, security monitoring, incident response, data hosting, support hours, restoration times and escalation arrangements.

5.5 Data Protection Officer

If the Council has a Data Protection Officer (DPO), the DPO should advise on data protection compliance and on personal data breaches. The DPO also advises on Data Protection Impact Assessments, privacy risks, and reporting obligations to the Information Commissioner's Office.

5.6 All users

All users must:

- comply with this policy and related procedures;
- use Council IT resources responsibly, lawfully and securely;
- protect devices, passwords, authentication methods and Council information;
- only access systems and data they are authorised to use;
- report incidents (IT problems or security issues), suspected breaches (possible leaks of information), loss, theft, compromise (unauthorised access or changes), phishing (fake messages trying to steal information) or unusual system behaviour immediately to the Proper Officer, who will, if necessary, report to the National Cyber Security Centre (NCSC) or Information Commissioner's Office (ICO);
- complete any required cybersecurity or data protection training;
- Return Council equipment, information and access credentials when their role ends.

6. Council Information Technology Systems

6.1 Personal use of Council IT

Is only allowed if it is reasonable, legal, and does not get in the way of Council work. It should not create security or reputational risks or cost the Council extra money.

Users must not use Council IT resources for:

- unlawful activity;
- harassment, bullying, discrimination or abuse;
- accessing, creating, storing or sharing offensive, obscene, extremist, hateful or otherwise inappropriate material;
- personal commercial activity;
- party-political campaigning, electioneering or activity that could improperly use Council resources;
- gambling, cryptocurrency mining or speculative activity unrelated to Council business;
- unauthorised copying, downloading or sharing of copyrighted material;
- any activity that could bring the Council into disrepute.

6.2 Email and messaging

All QTC employees and councillors will receive a Council email address. They must use this address for all Council business.

- use Council email accounts for Council business wherever accounts are provided;
- take care before opening attachments, clicking links or responding to unusual requests;
- verify requests for payment, bank detail changes, sensitive information or urgent action using a trusted second channel;
- avoid sending personal or confidential data by email unless necessary and appropriately protected;
- check recipients carefully before sending, especially where emails contain personal, confidential, financial or commercially sensitive information;
- not auto-forward Council email to personal accounts unless expressly approved and risk assessed;
- not use Council email for mass mailing unless lawful, appropriate and compliant with data protection and direct marketing requirements.

6.3 Internet use

Internet use must be lawful, appropriate and consistent with Council business. Users must not attempt to bypass Council security controls, filtering, monitoring or access restrictions.

6.4 Social media

Use of Council social media accounts is governed by the Council's Social Media Policy. Users must not use personal social media accounts in a way that improperly discloses Council information, breaches confidentiality, compromises data protection or gives the impression they are speaking on behalf of the Council without authority.

6.5 Public AI tools and external online services

Users must not enter personal data, confidential Council information, unpublished committee papers, legal advice, staff information, resident casework, financial information, security details, passwords, access codes or commercially sensitive information into public AI tools, translation tools, file conversion websites or other unapproved online services.
Approved tools may only be used where the Council is satisfied that data protection, confidentiality, retention, access control and supplier risks have been considered.

6.6 Portable devices and mobile working

Portable devices include laptops, tablets, mobile phones, USB drives, external hard drives, cameras, portable projectors and any other device capable of storing or accessing Council information.

Users must:

- Keep portable devices secure at all times;
- Use screen locks, passwords, PINs, biometrics or other approved authentication;
- Ensure devices are encrypted where they store or access Council information;
- Avoid leaving devices unattended in vehicles, public places, meeting rooms or community venues;
- Report loss, theft or suspected compromise immediately;
- Avoid storing Council information locally unless necessary;
- Transfer Council information to approved storage as soon as practicable;
- Securely delete local copies when no longer required;
- Avoid using untrusted chargers, cables or public charging points for Council devices unless suitable protection is used.

6.7 Personal devices / Bring Your Own Device

Personal devices may be used for Council work only if the Council permits it and the device is secure. Staff, councillors, volunteers, and trusted suppliers must email the Proper Officer for permission before connecting any personal device, such as a laptop, tablet, or smartphone, to the Council's network.

Where personal devices are used, users must:

- keep Council and personal data separate wherever possible;
- use strong device locking and up-to-date operating systems;
- install security updates promptly;
- not share the device account with family members or other users where Council data is accessible (using the same Laptop or desktop system is fine, providing separate accounts are used)
- not store Council files in personal cloud services unless expressly approved;
- allow Council data to be removed if access is withdrawn, the device is lost, or the user leaves office or employment;
- report loss, theft or compromise immediately.

The Council may refuse or withdraw permission to use personal devices where it considers the risk unacceptable.

7. Removable media

Use of removable media, including USB drives and external hard drives, should be avoided unless there is a clear business need and no safer alternative is available.
Where removable media is used for Council information, it must be approved, registered, encrypted, protected from loss, stored securely and securely wiped or destroyed when no longer required. Personal, confidential or sensitive information must not be stored on unencrypted removable media.

8. Passwords, authentication and access control

Users must protect passwords, passphrases, passkeys, authentication apps, security tokens and recovery codes.

The Council will:

- require unique accounts wherever practicable;
- avoid shared accounts unless there are documented needs and compensating controls;
- use multi-factor authentication for email, cloud services, finance systems, administrator accounts and any other high-risk systems wherever available;
- restrict administrator privileges to authorised users only;
- remove or disable accounts promptly when users leave or no longer require access;
- review user access periodically;
- encourage use of secure password managers where appropriate;
- Do not force password changes unless there is a suspected compromise or a system requires it.

Users must not:

- share passwords or authentication codes;
- write passwords where they can be found by others;
- reuse Council passwords on personal systems;
- approve unexpected multi-factor authentication prompts;
- attempt to access accounts, data or systems without authorisation.
- Network, device and software management

9. Asset management

The Council will maintain an inventory of key IT assets, including devices, accounts, software, licences, cloud services, websites, domain names, hosting arrangements, backup services and critical suppliers.

9.1 The inventory should record, where relevant:

- asset name or description;
- owner or assigned user;
- supplier or support provider;
- renewal dates;
- security or backup arrangements;
- whether the asset stores or processes personal, confidential or critical Council data.

9.2 Secure configuration

Council systems and devices should be configured securely before use. Default passwords must be changed. Unnecessary services, software and accounts should be removed or disabled. Devices should use encryption, automatic locking, malware protection and security settings proportionate to the risk.

9.3 Updates and patching

Operating systems, browsers, applications, plugins, firmware and security tools must be kept up to date. Unsupported or end-of-life software and devices must not be used for Council business unless a documented risk assessment and compensating controls are in place.

9.4 Software and licensing

Users must not install software, browser extensions, mobile apps or third-party tools on Council devices unless approved. Software must be properly licensed and obtained from trusted sources.

9.5 Malware protection

Council devices and systems should use appropriate malware protection, endpoint protection, email filtering, browser protection and security monitoring proportionate to the Council's risk profile.

Users must not disable security tools or ignore security warnings without the IT provider's or the Proper Officer's advice.

9.6 Network security

The Council will ensure that networks under its control are protected by appropriate measures, which may include firewalls, secure Wi-Fi configuration, strong passwords, guest network separation, logging, monitoring, access restrictions and supplier support arrangements.
Public or shared Wi-Fi should be avoided for sensitive Council work unless suitable protections are in place. Where necessary, users should use approved secure connections, trusted mobile data or other arrangements advised by the IT provider.

9.7 Cloud services and third-party systems

Cloud services and third-party systems must only be used where approved by the Council. Before adopting a new service, the Council should consider:

- what data will be stored or processed;
- where data is hosted;
- access controls and authentication;
- backup and export options;
- supplier security standards;
- contract terms;
- data protection requirements;
- business continuity arrangements;
- exit arrangements if the supplier changes or fails.

9.8 Disposal and reuse

Devices, storage media, and equipment must be securely wiped, destroyed, or returned to an approved supplier before being disposed of, recycled, sold, or reused. The Council must take reasonable steps to ensure Council information cannot be recovered from disposed equipment.

9.9 Monitoring and privacy

The Council may monitor the use of Council IT systems, devices and accounts where lawful, necessary and proportionate, including for security, audit, compliance, troubleshooting, investigating misuse, business continuity and protecting Council information.

Monitoring must comply with data protection and privacy requirements. Users should be informed that Council systems and accounts may be monitored. Monitoring should not be excessive and should be limited to legitimate Council purposes.

10. Incident reporting

10.1 What must be reported

Users must immediately report any actual or suspected IT, cybersecurity or data incident, including:

- lost or stolen devices;
- lost papers or removable media containing Council information;
- suspected phishing emails, suspicious links or unexpected attachments;
- malware, ransomware, pop-ups, unusual device behaviour or system warnings;
- unauthorised access to systems or accounts;
- accidental disclosure, misdirected emails or incorrect attachments;
- suspected compromise of passwords or multi-factor authentication;
- damaged equipment affecting Council systems or data;
- outage of critical systems;
- unauthorised software installation;
- any incident involving personal data;
- any event that may prevent the Council from delivering essential functions.

10.2 How to report

Incidents must be reported to the Proper Officer immediately via email and, where urgent, by phone, text, or WhatsApp message.

If the primary system is unavailable, users should use the alternative emergency contact route set out in the Council's incident contact list.

10.3 Immediate user actions

Users should:

- report the incident promptly, even if unsure;
- preserve evidence where possible;
- avoid deleting emails, files, logs or messages connected to the incident;
- disconnect a device from the internet or network if instructed, or where continuing connection appears to be causing active harm;
- not attempt their own technical investigation unless authorised;
- not communicate externally about the incident unless authorised.

10.4 Data breach assessment

Where an incident may involve personal data, the Clerk / Proper Officer must ensure it is assessed under the Council's Data Protection Policy and, where appropriate, with advice from the Data Protection Officer.

If a personal data breach is likely to result in a risk to individuals' rights and freedoms, the Council must consider whether it is reportable to the Information Commissioner's Office. Where reporting is required, it must be done without undue delay, normally within 72 hours of becoming aware of the breach. Where necessary, affected individuals must also be informed in accordance with UK GDPR.

10.5 External reporting

Depending on the nature of the incident, the Council may need to notify one or more of the following:

- IT provider;
- Data Protection Officer;
- Information Commissioner's Office;
- police or Action Fraud;
- National Cyber Security Centre reporting route;
- insurer;
- bank;
- website or cloud hosting provider;
- internal or external auditor;
- residents, staff, councillors, contractors or suppliers where appropriate;
- relevant principal authority, partner body or professional adviser.

The Clerk / Proper Officer, in consultation with the Chair, the relevant committee, the DPO, and the insurer or legal adviser, where appropriate, will determine external notifications.

11. Misuse of IT

Misuse includes any breach of this policy, including careless, negligent, deliberate or unlawful use of Council IT resources.

Examples include:

- accessing systems or data without authority;
- sharing passwords or authentication codes;
- attempting to bypass security controls;
- installing unauthorised software;
- using Council systems for unlawful, offensive or inappropriate activity;
- using Council resources for party-political campaigning, personal business or private gain;
- failing to protect Council information or devices;
- failing to report an incident promptly;
- deliberately deleting, altering or concealing Council records without authority;
- disclosing confidential or personal data without a lawful basis;
- using personal accounts or unapproved services to avoid Council records, retention or transparency requirements.

Suspected misuse may result in:

- withdrawal or restriction of IT access;
- investigation under staff disciplinary procedures;
- referral under the Councillor Code of Conduct arrangements;
- termination of contractor access or contract remedies;
- reporting to police, regulators or insurers where appropriate;
- recovery of costs where lawful and appropriate.

The Council will act fairly and proportionately, considering intent, risk, harm, previous conduct, and whether the user reported the matter promptly.

12. Backup and retention

12.1 Records and retention

Council records must be retained and disposed of in accordance with the Council's Data Retention Policy. Backup systems are not a substitute for proper records management. Users must not use backups as informal archives or to keep records beyond agreed-upon retention periods.

12.2 Backup principles

The Council will ensure that key systems and critical Council data are regularly and securely backed up. Backup arrangements should be proportionate to the importance of the data and the impact of loss.

Backup arrangements should include:

- identification of key systems and data requiring backup;
- clear responsibility for backup management;
- backup frequency appropriate to operational need;
- encryption or other suitable protection;
- protection against ransomware or accidental deletion;
- storage separate from the live system where practicable;
- periodic testing of restoration;
- documented recovery steps;
- consideration of supplier responsibilities for cloud systems.

13.3 Restoration testing

The Council should test its ability to restore important files, systems or records at reasonable intervals and after significant system changes. Failed tests or restoration issues must be logged and addressed.

13.4 Backup access

Access to backups must be restricted to authorised persons. Backup administrator accounts must be strongly protected and should use multi-factor authentication where available.

13. Crisis management and major disruption

13.1 Definition of a major IT crisis

A major IT crisis is any incident that materially affects the Council's ability to operate, protect data, pay suppliers or staff, communicate with residents, access statutory records, manage bookings, administer meetings, maintain financial controls or deliver essential services.

Examples include:

- ransomware or destructive malware;
- compromise of Council email or administrator accounts;
- major data breach;
- fire, flood, electrical damage or theft affecting IT equipment or records;
- failure of a critical supplier, cloud service, website, finance system or storage provider;
- loss of access to key records or backups;
- prolonged power, internet or premises outage;
- suspected hostile or criminal attack on Council systems.

13.2 Crisis objectives

In a major IT crisis, the Council's objectives are to:

- Protect people and public safety.
- Contain the incident and prevent further harm.
- Protect personal, confidential and critical Council data.
- Maintain essential Council functions using manual or alternative arrangements where necessary.
- Communicate clearly with councillors, staff, residents, suppliers, regulators and partners.
- Restore systems and data safely.
- Preserve evidence and support any investigation.
- Learn lessons and improve controls.

13.3 Initial crisis actions

The Proper Officer, or a nominated deputy, should coordinate the initial response. The Council should:

- confirm the nature and scale of the incident;
- contact the IT provider and relevant senior councillors;
- activate emergency contact arrangements if normal systems are unavailable;
- preserve evidence and avoid unnecessary changes to affected systems;
- isolate affected systems where advised or necessary;
- assess whether personal data is involved;
- assess whether essential Council functions can continue;
- consider notifying insurers, ICO, NCSC, police, bank or other bodies as appropriate;
- agree on internal and external communications;
- maintain a written incident log.

13.4 Emergency operating arrangements

The Council should maintain basic arrangements that allow essential business to continue if IT systems are unavailable, including:

- offline or printed emergency contact list;
- alternative method for contacting councillors and staff;
- access to key supplier and IT provider details;
- alternative arrangements for urgent payments and banking controls;
- copies of key policies, insurance details and business continuity procedures;
- manual meeting administration arrangements where lawful and practical;
- alternative access to essential documents required for statutory deadlines.

13.5 Communications during a crisis

Only authorised persons, such as the Proper Officer or their nominated deputies, may issue external communications about a major IT incident. Communications should be accurate, timely, and calm, and should avoid speculation. Where information is incomplete, the Council should say what is known, what is being done and when further updates are expected.

Communications may need to cover:

- councillors and staff;
- residents and service users;
- hirers, suppliers and contractors;
- principal authorities or partner organisations;
- regulators;
- media enquiries;
- website and social media updates.

13.6 Recovery

Systems must not be restored until the Council and its IT provider are satisfied that restoration is safe, secure, and that the cause of the incident has been understood and addressed to reduce the risk of immediate reinfection or repeat failure.

Recovery should prioritise:

- safety and legal obligations;
- financial controls and banking;
- statutory records and meeting administration;
- email and communications;
- website and public information;
- bookings, community building systems and operational services;
- routine administrative systems.

13.7 Post-incident review

After any significant incident, the Council should conduct a review covering:

- what happened;
- when it was detected;
- what systems, data and services were affected;
- what decisions were made and by whom;
- whether reporting obligations were met;
- what worked well;
- what needs improvement;
- whether policies, contracts, backups, training or technical controls need to change.

The findings should be reported to the Council or relevant committee, excluding confidential or security-sensitive details where necessary.
Training and awareness

The Council will ensure that users receive proportionate guidance on safe IT use, phishing, passwords, multi-factor authentication, device security, data protection and incident reporting.
Training may include formal training, briefings, written guidance, simulated exercises, reminders or discussion at induction. Users should be reminded that cybersecurity is not solely a technical matter and that prompt reporting is essential.

14. Suppliers and third parties

The Council will take reasonable steps to ensure that suppliers who provide IT, hosting, cloud, software, website, payment, finance or data processing services have appropriate security and data protection arrangements.

Where relevant, contracts should address:

- data protection roles and responsibilities;
- confidentiality;
- access controls;
- backup and restoration;
- incident reporting timescales;
- security standards;
- audit or assurance rights;
- subcontracting;
- data location;
- exit and data return arrangements;
- business continuity;
- insurance.

For higher-risk suppliers, the Council should consider whether Cyber Essentials, Cyber Essentials Plus or equivalent assurance is required.

15. Review

This policy will be reviewed at least annually, or sooner if:

- there is a significant IT or cyber incident;
- official guidance or legislation changes;
- the Council introduces major new systems;
- there is a change of IT provider;
- audit, insurance, DPO or professional advice recommends review;
- Council structure, staffing, or services materially change

All staff, councillors, and relevant users will be notified of any policy updates, urgent changes or critical new requirements. Communication will be via a briefing at Full Council to ensure maximum awareness and compliance. Where possible, a summary of significant changes will be provided.

Approval

This policy was approved by Full Council on DD/MM/YYYY

Signed: _____

Name: Cllr Shane Wilcox

Role: Chair

Date: 17/08/26

Minute Ref: FC-072/26-27

Appendix A: Minimum operational controls checklist

This checklist assumes full compliance. Some items may not apply or doing them may not always significantly reduce risks.

Control area	Minimum expectation	Evidence / owner
Asset register	Key devices, systems, accounts, suppliers and cloud services are recorded	[Insert]
Access control	Users have role-appropriate access only	[Insert]
Leavers process	Accounts and access are removed promptly	[Insert]
Multi-factor authentication	Enabled for email, finance, cloud and admin accounts where available	[Insert]
Updates	Devices and software are patched, and unsupported systems are identified	[Insert]
Malware protection	Suitable protection is enabled and monitored	[Insert]
Backups	Critical data is backed up and protected from ransomware	[Insert]
Restore testing	Backup restoration is tested periodically	[Insert]
Incident contacts	The emergency contact list is available offline	[Insert]
Training	Users receive proportionate cyber and data protection guidance	[Insert]
Supplier assurance	Key suppliers have security and data protection arrangements	[Insert]
Policy review	Policy reviewed annually or after major changes/incidents	[Insert]