KNOWSLEY TOWN COUNCIL

Information Technology & Digital Use Policy

Approved: 19/02/2026
Review Date: 20/02/2028
Applies to: All members, officers, and authorised users

Index

Knowsley Town Council

INFORMATION TECHNOLOGY, DIGITAL USE & SOCIAL MEDIA POLICY

Purpose

The purpose of this policy is to ensure that all Information Technology (IT), digital systems, data and social media platforms used by Knowsley Town Council are used **legally, securely, responsibly and professionally**.

This policy protects:

- The Council's data and information
- The Council's reputation
- Compliance with legal and regulatory requirements
- Members and Officers using digital systems

1. Scope

This policy applies to:

- Elected and co-opted Members
- The Clerk/RFO and all staff
- Contractors, volunteers and authorised third parties

It covers:

- Council-owned IT equipment and systems
- Personal devices used for Council business (BYOD)
- Email, digital communications and cloud systems
- Social media and online engagement
- Handling of personal and confidential data

2. Legal & Regulatory Framework

This policy supports compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
- Accounts and Audit Regulations 2015
- SAPPP Practitioners' Guide 2025 – **Assertion 10 (Digital & Data Compliance)**

4. Acceptable Use

All users must:

- Use Council IT systems for official Council business only
- Act lawfully, professionally and respectfully at all times
- Protect confidential and personal information
- Follow this policy and any related procedures

Users must **not**:

- Access or distribute offensive, illegal or inappropriate material
- Use Council systems for party political purposes or private business
- Bring the Council into disrepute through digital activity

5. Email & Digital Communications

- Only Council-issued email accounts must be used for Council business
- Personal email accounts (e.g. Gmail, Hotmail) must not be used
- Sensitive or personal data must be encrypted or shared securely
- Users must not impersonate others or imply authority they do not have

6. Passwords & Access Control

- Strong, unique passwords must be used and kept confidential
- Devices must be locked when unattended
- Login details must never be shared
- Suspected breaches must be reported immediately to the Clerk/RFO

7. Cybersecurity

Users must:

- Be vigilant against phishing and suspicious links
- Keep devices updated with antivirus and security patches
- Report cybersecurity incidents or data breaches immediately

The Clerk/RFO is responsible for coordinating any response, including reporting to the ICO where required.

The Council will ensure that appropriate arrangements are in place for the secure backup of Council data and systems to support business continuity and data recovery in the event of system failure, cyber-attack or data loss.

8. Members' Digital Conduct & Responsibilities

Councillors have additional responsibilities under the Code of Conduct.

- Digital communications may create implied authority or legal obligations

- Misuse of IT systems or inappropriate digital conduct may be referred to the Monitoring Officer
- Members must take care when using email, messaging or online platforms in their role as councillors

9. Use of Personal Devices (BYOD)

Personal devices may only be used for Council business with approval from the Clerk/RFO.

Requirements:

- Devices must be password-protected and secure
- Council data must not be stored permanently on personal devices
- Council data must be deleted when no longer required

10. Remote Working

- Secure connections (e.g. VPN) must be used on public networks
- Devices must be always kept secure
- Paper records must be stored and disposed of securely
- The same standards apply as if working in the office

11. Data Protection & Freedom of Information

All users must:

- Handle personal data lawfully, fairly and securely
- Only share data where authorised
- Comply with data retention and disposal requirements
- Be aware that Council information may be subject to FOI requests

Subject Access Requests, data breaches and retention matters must be referred to the Clerk/RFO.

12. Social Media Use (Council Accounts)

- Only authorised Members or Officers may post on behalf of the Council
- Content must be factual, neutral and professional
- Political content, arguments or inflammatory posts are not permitted
- Council accounts must be monitored regularly

13. Personal Use of Social Media

When acting as a councillor:

- Users must not bring the Council into disrepute
- Confidential information must never be shared
- Personal opinions must be clearly distinguished from Council business

- Online behaviour may still be subject to complaints or FOI

14. Training & Awareness

- Annual IT and digital security training will be provided
- New Members will receive digital governance guidance
- Ongoing support is available from the Clerk/RFO

15. Breaches & Enforcement

Breaches of this policy may result in:

- Disciplinary action (staff)
- Referral to the Monitoring Officer (Members)
- Reporting to the Information Commissioner's Office (ICO)

Examples include:

- Sharing passwords
- Misuse of systems
- Insecure handling of Council data

Use of Council IT systems may be monitored or reviewed where necessary for security, audit, investigative or compliance purposes, in accordance with data protection legislation.

16. IT Equipment and Asset Management

All Council-owned IT equipment, including laptops, tablets, mobile phones and storage devices, remains the property of Knowsley Town Council at all times.

IT equipment must be used only by the individual to whom it is issued and must not be shared.

All equipment must be returned immediately upon request, or when a Member leaves office, an employee leaves employment, or access is withdrawn.

The Clerk/RFO is responsible for maintaining an inventory of Council IT equipment and ensuring its secure issue, return and disposal.

16. Use of Borough Council IT Systems

Where IT services are provided under a Service Level Agreement with Knowsley Metropolitan Borough Council, users must also comply with the Borough's **Acceptable Use of IT Policy**.

17. Review

This policy will be reviewed annually or sooner if legislation, technology or Council operations change.

Agreed by Knowsley Town Council on:

Minute Reference: