TORPOINT TOWN COUNCIL

ICT / ICT & DATA COMPLIANCE POLICY

RENEWAL DATE: - October 2025

NEXT RENEWAL DATE: - June 2027

Reviewing Body: -

Contents

1. Purpose

This policy sets out how Torpoint Town Council manages its information technology, digital systems, website, email, and social media in a secure, lawful, transparent and accountable way. It ensures the Council complies with Assertion 10 (Digital and Data Compliance) of the Annual Governance and Accountability Return (AGAR) 2025/26, and protects the Council, its members, staff, and residents.

2. Scope

This policy applies to:

- All councilors, employees, volunteers, and contractors working on behalf of the Council.
- All Council-owned ICT systems, devices, email accounts, software, and cloud services.
- Any personal devices used to conduct Council business.
- The Council's official website and social media accounts managed by the Town Council's administration team under the direction of the Town Clerk / RFO.
- All personal data collected, stored, processed, or shared by the Council in any form.

3. Legal and Regulatory Framework

Torpoint Town Council will comply with:

- UK General Data Protection Regulation (UK GDPR) *(UK Government, 2018b)*
- Data Protection Act 2018 (UK Government, 2018a)
- Freedom of Information Act 2000 *(UK Government, 2000)*
- Local Government Transparency Code 2015 (where applicable)*(UK Government, 2015)*
- The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018(UK Government, 2018c)
- Web Content Accessibility Guidelines (WCAG) 2.2 AA standard *(Web Accessibility Initiative, 2024)*
- The Misuse of computers Act 1990 *(UK Government, 1991)*
- Other relevant laws, regulations and proper practices as updated from time to time.

4. Website and Social Media

4.1 Domain and Email

- All Council business shall be conducted using the official domain **torpointtowncouncil.gov.uk**.
- Councillors and staff must use Council-issued email accounts for all official correspondence.
- Council email systems are externally supplied and supported by Western Web Computer Systems and are backed up externally for 30 days.
- Any suspicious emails or suspected security breaches should be reported to the Town Clerk / RFO, or her team immediately.
- Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.
- No attachments of unknown origin are to be opened, and all such correspondence should be reported to the Town Clerk / RFO, or her team immediately.

4.2 Website

- The Council's website is managed by the Torpoint Town Council administration team under the guidance of the Town Clerk.
- It must comply with the Accessibility Regulations 2018 and WCAG 2.2 AA standards and be tested for compliance every two years. (We do not currently meet this as we are only checked to 2.1 AA , however Western web have confirmed that they have applied the 2.2 update and so a test is needed)
- Where full compliance is not yet possible, an Accessibility Statement will be published and kept under review. *(Torpoint Town Council, 2020)*
- All statutory information must be published promptly and must include:
    - Agendas
    - Minutes
    - Policies
    - Accounts
    - transparency code
    - data compliance

4.3 Social Media

- The Council's social media accounts are managed by the Torpoint Town Council administration team under the guidance of the Town Clerk.
- All content must be professional, accurate, and reflect Council decisions and policies only.
- The Council will present a neutral stance on all public matters outside of their control, unless a democratic vote of the council directs the Clerk to do otherwise.
- Personal accounts must not be used for official Council business.

Current social media accounts belonging to the council are:

- Facebook
    - Torpoint Town Council *(Torpoint Town Council, 2025b)*
    - Torpoint Library and Community Hub *(Torpoint Town Council, 2025a)*
- WhatsApp – The Town Council maintains a private Whatsapp group for council members only and is maintained and controlled by the Town clerk.
- Youtube (Torpoint Town Council, n.d.)
- Instagram *(Torpoint Library and Community Hub, n.d.)*

5. Data Protection

Please see Torpoint Town Council's Data Protection policy for further details. (Torpoint Town Council, 2023)

5.1 Data Controller

- Torpoint Town Council is the Data Controller with delegated authority given to the Town Clerk / RFO.
- The Town Clerk / RFO is designated as the Council's Data Protection Officer (DPO).
- Where there is potential for a conflict of interest in the Clerk / RFO carrying out the role of Data Protection Officer, responsibility will revert to the Town Council for direction.

5.2 Principles

Personal data must be:

- Processed lawfully, fairly and transparently.
- Collected only for specified purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Retained only as long as necessary.
- Secured against loss, misuse, or unauthorised access.

5.3 Registers and Audits

- The Council shall maintain a record of personal data held, why it is held, how it is processed, retention periods, and disposal methods.
- Regular audits of data held will be carried out.

5.4 Rights of Individuals

- The Council shall publish a Privacy Notice explaining how personal data is used.
- Data Subject Access Requests (DSARs) will be managed in line with statutory timescales.

5.5 Breach Reporting

- Any data or security breach must be reported immediately to the Clerk / RFO.
- The Town Clerk / RFO will assess and, if necessary, report breaches to the Information Commissioner's Office (ICO).

- Where there is potential conflict of interest in the Clerk / RFO carrying out such tasks, responsibility will revert to the Town Council for direction.

6. ICT Security and Acceptable Use

6.1 ICT Support

- All ICT support enquiries and problems should be directed to the Town Council's Administration team under the control of the Town Council and RFO.
- Some of the Council's IT systems are supported in part by Western Web an external contractor. (Western Web, 2025)
- **Security updates** are not externally supported and it is the responsibility of the Town Clerk / RFO to ensure that all required security updates are applied to Torpoint Town Council systems and devices.
- **Virus Protection** is not externally supported and it is the responsibility of the Town Clerk / RFO to source and maintain across all Torpoint Town Council systems and devices.

6.2 Acceptable Use

- Council-owned devices and systems are provided for Council business.
- Personal use of Council devices and systems is not permitted without prior approval from the Town Clerk / RFO and must not interfere with Council operations.
- No unauthorised software or apps may be installed on Council devices.

6.3 Passwords and Access

It is the responsibility of the Town Clerk and RFO to ensure that all Council systems are secure and appropriate access given to council users, employees, members and external contractors.

- Strong passwords must be used on all systems and devices.
- Passwords and system access must not be shared.
- Passwords must not be written down in plain text
- Access to sensitive data is restricted to authorised users only.
- Two Factor authentication options should be chosen when available, unless this would cause organisational difficulties in accessing systems.
- Mobile devices provided by Torpoint Town Council must be secured with passcodes and/or biometric authentication where possible.
- No person shall try to access, or read Town Council systems which they do not have access to, or which their level of access does not allow.

6.4 Personal Devices

- Where personal devices are used for Council business, they must be password-protected, up to date with security patches, and only used for work in accordance with this policy.
- Sensitive Council data must not be permanently stored on personal devices.

6.5 Backups and Continuity

- All Council data shall be backed up securely and regularly.
    - The Town council is supported with the support of Western Web, and consists of a fixed office-based file server linked to a cloud-based service for redundancy back up. (This is not currently working and Western Web need to fix this)
- Torpoint Library and Community Hub's ICT systems are maintained and supported by Cornwall Council under agreement with Torpoint Town Council.

All relevant data backup, security updates, virus protection and ICT support for Torpoint Library and Community Hub are maintained and delivered by Cornwall Council under the direction of the Town Clerk / RFO.

- A continuity plan is in place to manage disruption of ICT systems to Torpoint Town Council in cases of emergency, damage, sabotage or external interference.
- It is the responsibility of the Town Clerk / RFO to ensure that all council owned and used devices are fit for purpose and that they do not represent a risk to Council owned systems or the security of data due to age or condition. This includes:

    - Outdated operating systems e.g. Microsoft Windows or Mac OS
    - Outdated Software packages which have security flaws.
    - That sufficient Virus protection software and firewall systems are in place to safeguard the Town Council and its data.

6.5 Network and internet usage

- Torpoint Town Council's internal / external network, and it's internet connections must be used responsibly and efficiently for official purposes only.
- The downloading and sharing copyrighted material without proper authorisation are prohibited.
- Public access to guest WIFI is permitted, however the downloading of copyrighted, illegal or obscene material is prohibited, and we reserve the right to inform law enforcement agencies if we detect any illegal activity on Town Council devises, network or WIFI.

7. Roles and Responsibilities

- Full Council: Adopts this policy, monitors compliance through the AGAR process, and ensures adequate resources are available.
- Clerk / RFO (DPO): Responsible for day-to-day implementation of this policy, ensuring compliance, training, handling data protection matters, and reporting breaches.
- Administration Team: Manages the website and social media, ensuring compliance with accessibility and transparency requirements.
- External IT Contractor: Provides technical support and advise where required.
- Town Clerk / RFO ensures Council systems and devices are secure, backed up, up to date and fit for purpose.
- Councillors and Staff: Must comply with this policy, use Council systems responsibly, and report any concerns or breaches to the Town Clerk / RFO.
- The Town Clerk / RFO is responsible for ensuring that all employees and councillors receive initial, essential and regular training on all aspects of data security, best practice, and Torpoint Town Council policies and procedures.

8. Monitoring and Review

- This policy shall be reviewed annually, or earlier if legislation, guidance, or Council operations change.
- Evidence of compliance will be presented to Internal Audit and used to support the Council's response to Assertion 10 of the AGAR.
- The Town Council maintains an asset register containing all ICT devices which is updated regularly.
- Torpoint Town Council reserves the right to monitor email communications. This is to ensure compliance with this policy and all relevant laws. It is the responsibility of the Town Clerk / RFO to conduct such searches.
- Monitoring will be conducted in accordance with the Data Protection Act and GDPR. It is the responsibility of the Town Clerk / RFO to conduct such searches, but may ask Western Web communications to carry out any searches of archived / backed up emails on their behalf.
- If the Town Clerk is ever conflicted in their duty to carry out the duties defined above, then the deputy Town Clerk / Town Clerks assistant will carry out such tasks required.

9. Non-Compliance

Failure to comply with this policy may result in disciplinary action for staff, referral to standards bodies for councillors, and/or legal action where data protection law has been breached.

Please see Torpoint Town Council's Employee Handbook and Officer / Member Protocol policy for further details (Torpoint Town Council, 2018)

10. Evidence for AGAR Assertion 10

The Council will retain and make available for audit:

- This adopted ICT / IT & Data Compliance Policy.
- Published Privacy Notices and Accessibility Statement.
- Records of data protection training for staff and councillors.
- Evidence of secure domain, email, backups, and IT contractor arrangements.
- Records of data audits, retention schedules, and any DSARs or breaches handled.

Bibliography

Torpoint Library and Community Hub. (n.d.). *Torpoint Library and Community Hub Instagram* . Https://Www.Instagram.Com/Torpointlibraryandcommunityhub/.

Torpoint Town Council. (n.d.). *Torpoint Town Council Youtube Page*. Https://Www.Youtube.Com/Channel/UCH_lNCZGfDcmxlsyZW8G4wA?View_as=subscriber.

Torpoint Town Council. (2018, October). *Torpoint Town Council Employee Handbook and Officer / Member Protocol*. Https://Www.Torpointtowncouncil.Gov.Uk/Data/Uploads/2824_748832321.Pdf.

Torpoint Town Council. (2020, September 20). *Torpoint Town Council Accessibility Statement*. Https://Www.Torpointtowncouncil.Gov.Uk/Accessibility-Statement.Php.

Torpoint Town Council. (2023, June). *TORPOINT TOWN COUNCIL DATA PROTECTION, PLUS DOCUMENT RETENTION & DISPOSAL POLICY*. Www.Torpointtowncouncil.Gov.Uk.

Torpoint Town Council. (2025a). *Torpoint Library and Community Hub Facebook Page*. Https://Www.Facebook.Com/Torpointlibrary.

Torpoint Town Council. (2025b). *Torpoint Town Council Facebook Page*. Https://Www.Facebook.Com/Torpointtowncouncil.Gov.Uk.

UK Government. (1991, February 1). *Computer Misuse Act 1990*. Https://Www.Legislation.Gov.Uk/Ukpga/1990/18/Contents#:~:Text=Computer%20Misuse%20Act%201990%20is%20up%20to%20date,Site%20may%20not%20be%20fully%20up%20to%20date.

UK Government. (2000, November 30). *Freedom of Information Act 2000*. Https://Www.Legislation.Gov.Uk/Ukpga/2000/36/Contents.

UK Government. (2015, February 27). *Local Government Transparency Code 2015*. Https://Www.Gov.Uk/Government/Publications/Local-Government-Transparency-Code-2015/Local-Government-Transparency-Code-2015.

UK Government. (2018a, May 23). *Data Protection Act 2018*. Https://Www.Legislation.Gov.Uk/Ukpga/2018/12/Contents/Enacted.

UK Government. (2018b, June 25). *UK General Data Protection Regulation (UK GDPR)*. Https://Www.Legislation.Gov.Uk/Eur/2016/679/Contents.

UK Government. (2018c, September 23). *The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018*. Https://Www.Legislation.Gov.Uk/Uksi/2018/952/Contents.

Web Accessibility Initiative. (2024, December 12). *Web Content Accessibility Guidelines (WCAG) 2.2*. Https://Www.W3.Org/TR/WCAG22/.

Western Web. (2025). *Western Web Computer Services*. Https://Www.Westernweb.Uk/Computers.Php.