Integrated Data and IT Policy

Policy Administration	
Adopted:	Jan 2026 (Previously Data Protection Policy)
Approved By:	Newbiggin Town Council
Minute Reference:	C109/25
Responsible Officer:	Town Clerk & RFO
Review Frequency:	Annually (Rev in March 26), now V3
Next Review of Policy:	March 2027 (Or earlier if required)

Integrated Data and IT Policy

Introduction and Purpose

Newbiggin by the Sea Town Council is committed to protecting personal data and using information technology securely and responsibly. As a public authority, the Council acts as a data controller under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

This single integrated policy replaces the existing outdated Data Protection Policy (based on the repealed Data Protection Act 1998) and introduces a new IT Policy. It ensures compliance with current law and the Practitioners' Guide 2025 (Assertion 10: Digital and Data Compliance) for the 2025/26 Annual Governance and Accountability Return.

The policy applies to all councillors, employees, volunteers, contractors, and any other authorised users, regardless of location or device used (including personal devices accessing Council systems).

Key Principles

The Council will process personal data and manage IT in line with UK GDPR principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

IT-specific measures include:

- Use of Council-owned.gov.uk email addresses for all official communication
- Multi-factor authentication (MFA) where available
- Encryption for sensitive data
- No unauthorised software or personal storage devices without approval

Responsibilities

- **Town Clerk** (designated lead for data protection and IT): Monitors compliance, handles requests and breaches, provides advice, liaises with the Information Commissioner's Office (ICO), conducts audits, and arranges training.
- **All users**: Must follow this policy, report incidents immediately, and complete annual training.
- **Third-party processors** (e.g. website/email hosting provider): Must have a written Data Processing Agreement (DPA) meeting Article 28 UK GDPR requirements and provide equivalent security.

Data Handling and IT Usage

Collection and Processing

Personal data will only be collected where necessary and processed on a lawful basis (e.g. legal obligation, contract, legitimate interests, consent). Privacy notices will be provided where required. High-risk processing will involve a Data Protection Impact Assessment (DPIA).

Storage and Security (Article 32 UK GDPR)

- Data will be stored securely using encryption, access controls, regular backups, and secure disposal.
- Devices must be locked when unattended; portable devices must not be left in vehicles or unattended.
- Sensitive data must not be sent by email unless encrypted.
- Strong passwords (preferably three random words) and MFA if required.

Information Security and Confidentiality

Councillors and officers must not forward council information to personal email accounts or store council data on personal devices unless authorised and secured. Confidential information, including personal data or commercially sensitive information, must not be shared in accordance with council procedures.

Email, Internet, and Social Media

- Official communication must use Council.gov.uk email addresses only.
- Emails must be professional; verify attachments/links to avoid phishing.
- Internet use is for official purposes, no unauthorised downloads.
- Social media engagement is encouraged for Council purposes, but must be relevant and professional. No abusive, discriminatory, or derogatory posts (even personal ones that could harm the Council's reputation) will be tolerated – such behaviour may lead to disciplinary action.

Acceptable Use of Council Email

Council-issued email accounts are provided to councillors and officers to conduct official council business.

These accounts must not be used for:

- Personal business activities
- Unauthorised political campaigning
- Distribution of inappropriate, offensive, or unlawful material
- Sharing confidential Council information without proper authorisation.

Limited incidental personal use may be permitted, provided it does not interfere with council duties or create security or reputational risks for the Council.

Laptop and Device Use (Work From Home/Meetings)

Council laptops and IT equipment are provided for official council duties, including: -

- Working from home
- Attending meetings, conferences, or training
- Accessing council systems and documents remotely.

Users must ensure that: -

- Devices are password-protected
- Screens are not visible to unauthorised persons when working in public places
- Devices are not left unattended in insecure locations
- Council data is stored only on approved systems
- Lock Screens when away from the device
- Use secure Wi-Fi or VPN

- Report lost or theft of devices immediately

Remote Working Expectations

For officers working from home: -

Officers working remotely must ensure that council data remains secure and that devices provided by the Council are used only for the authorised council work, using the system in place to access remotely which is also password protected.

Access Termination and Return of Council IT Equipment

All council equipment must be returned immediately upon termination of employment or end of office. This included but not limited to: -

- Council issued laptops
- Mobile phones or tablets (None currently)
- Storage devices (USB drives, external hard drives)
- ID Badges and keys
- Any other IT and electronic equipment issued by the Council

Equipment should be returned to the Town Clerk or designated officer before the individual's final working day or immediately following the end of their term of office.

Passwords and Access Credentials

Before departure, officers must provide the Town Clerk or designated officer with access to any council systems or accounts for which they hold administrative responsibility. This may include: -

- Shared account passwords
- System administrative credentials
- Access to cloud storage systems or shared drives
- Website administrative accounts not already shared

Following departure, all passwords associated with those accounts must be changed as soon as practicable.

Termination of Email Accounts

Where a Councillor or officer has been issued with a council email address (including government or council domain accounts), the following actions will take place: -

- The account will be deactivated or terminated with the email provider once the individual has left office or employment. If the accounts are office-based with the generic Town Clerk and Admin Assistant, then passwords will be changed immediately.
- The Council may retain the email account for a short period where necessary for administrative purposes, subject to data protection requirements.
- An automatic response or forwarding arrangement may be temporarily set up to direct enquiries to the appropriate council contact.
- Access to the account will be removed immediately upon termination.

All actions must be undertaken in compliance with the UK General Data Protection Regulation and the Data Protection Act 20218.

Integrated Data and IT Policy

Council Communications

Councillors and Officers must use their official council-issued email accounts for conducting council business wherever possible. This ensures transparency, proper record keeping, and compliance with data protection requirements.

Council business should not normally be conducted using personal email accounts.

Restrictions to Personal Email Use

Personal email accounts must not be used to:

- Send or receive confidential council information
- Share personal data relating to residents, staff, or contractors
- Circulate council documents that are not already publicly available
- Conduct formal council decision-making or official communications

Record Keeping

All Council-related communications must be capable of being retained as part of the council's official records in accordance with the council's data retention and records management procedures.

Failure to ensure proper record keeping may result in difficulties responding to requests under the Freedom of Information Act 2000 or the Data protection Act 2018.

Use of Messaging Applications and Information Communication Channel - Acceptable Communication Platforms

Messaging applications such as WhatsApp, text messaging, or other informal communication platforms are occasionally used for administrative or logistical purposes only, such as: -

- Confirming meeting times
- Sharing publicly available information
- Arranging attendance at events or meetings

These platforms should not be used to conduct council decision-making or formal discussions relating to council business.

Restrictions

Messaging applications must not be used for:

- Discussing confidential or sensitive council matters
- Sharing personal data relating to residents, staff, or contractors
- Making decisions that should properly be made at a council meeting
- Circumventing the council's formal decision-making processes

Where council business is discussed via informal messaging platforms, a record of the relevant information should be transferred to the council's official systems where appropriate.

Transparency and Governance

Councillors should be mindful that communications relating to council business may still be subject to disclosure under the Freedom of Information Act 2000 and relevant data protection legislation.

Good governance requires that official council discussions and decisions be conducted through appropriate formal channels.

Councillors should avoid forming informal groups on messaging platforms that could give the appearance of conducting business or decision-making outside properly convened council meetings.

Monitoring

The Council reserves the right to monitor IT use proportionately and in compliance with privacy laws (e.g. for security or policy enforcement).

The Council reserves the right to monitor or review the use of Council email accounts where there is a reasonable concern regarding misuse.

Monitoring may be carried out where this suspicion of:

- Unauthorised sharing of confidential or sensitive information
- Breaches of council policies#
- Misuse of council systems for personal or commercial purposes#
- Potential legal, security, or reputational risks to the Council

Monitoring activities will be undertaken proportionally and in accordance with guidance from the Information Commissioner's Office and the Council's obligations under the UK General Data Protection Regulation and the Data Protection Act 2018.

Rights and Requests

- **Subject Access Requests (SARs)** and other rights (rectification, erasure, restriction, portability, objection): Free of charge, responded to within one month (extendable for complexity).
- **Freedom of Information requests**: Forwarded to the Town Clerk; the Council complies with its Publication Scheme and the Local Government Transparency Code.

Breaches and Incidents (Articles 33 & 34 UK GDPR)

- Any suspected personal data breach or IT security incident must be reported to the Town Clerk immediately.
- The Town Clerk will assess risk and, if required, notify the ICO **within 72 hours** of awareness (unless unlikely to risk individuals' rights).
- Affected individuals will be informed without undue delay if the breach poses a 0
- high risk.
- All incidents (reportable or not) will be documented internally.

Any suspected misuse of council IT systems may be investigated. Breaches of this policy may result in appropriate action in accordance with council procedures and relevant legislation.

Failure to comply with this policy may result in investigation and appropriate action by the Council. If the communication relates to council business, it must be capable of being recorded on council systems.

Training, Audits, and Review

- Annual training on data protection, cybersecurity, and this policy will be provided.
- Annual data and IT audits will be conducted.
- This policy will be reviewed annually or following significant legislative/technological changes.

Definitions

- **Personal Data**: Any information relating to an identified or identifiable living individual.
- **Special Category Data**: Sensitive data (e.g. health, ethnic origin) requiring stricter conditions.
- **Processing**: Any operation on personal data (collection, storage, use, deletion, etc.).
- **Data Breach**: A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- **Data Controller**: The Council, determining purposes and means of processing.
- **Data Processor**: External provider processing data on the Council's behalf.