Appleby-in-Westmorland Town Council

IT Policy

The Purpose of the IT Policy

The purpose of Appleby Council's IT policy is to establish clear parameters for how Councillors and staff use council-provided technology or equipment in the course of their duties, including:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

Scope of this Policy

This policy applies to all councillors, staff, and other authorised users, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer use

Hardware

1. Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the Chair and Town Clerk). Any personal use of our computers and systems should not interrupt council work in any way. Staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.
2. Staff, and other authorised users, must lock their computers when leaving their desks for a prolonged period and should be properly closed down at the end of the day to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.
3. All computer and other electronic equipment supplied should be treated with good care at all times and any damage sustained to any equipment will have a financial impact on the council.

4. All computer and other electronic equipment supplied should be treated with good care at all times and any damage sustained to any equipment will have a financial impact on the council.
5. Equipment should not be dismantled or reassembled without seeking advice. Any faults or necessary repairs must be reported to the Town Clerk.
6. Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software) unless previously authorised.

Equipment – Portable Equipment

1. Portable equipment includes laptop computers, tablets, mobile and smart phones with email capability and access to the internet etc.
2. All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.
3. It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Any security set on these devices must not be disenabled or removed.
4. If an item of portable equipment is lost or damaged this should be reported to the Town Clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the costs of the loss/damage.
5. Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).
6. In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Town Clerk.

Use of Personal Equipment

1. The Council recognises that councillors may wish to use their own smartphones, tablets, laptops etc to access their emails and any documents sent to them via email. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately updated.
2. The same security precautions apply to personal devices as to the council's desktop equipment. Any emails sent from personal devices should be sent from council email accounts and should not identify personal email addresses.
3. Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). An example would be downloading copyright music illegally or accessing pornographic material.
4. Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports

both work and personal profiles, the work profile must always be used for work-related purposes.

5. Councillors and staff who intend to use their own devices via the council's infrastructure must ensure that they:
   - Use a strong password or facial / fingerprint to protect their device.
   - Ensure all Wi-Fi networks that are used are private and secure.
   - Ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device.
   - Inform the Clerk if any device containing work-related data is lost, stolen, or inappropriately accessed where there is risk of access to council data or resources.
6. Personal data relating to councillors or staff should not be saved to any personal accounts with third-party storage cloud service providers, as this may breach data protection legislation or create a security risk if the device is lost or stolen.
7. Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.
8. If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.
9. Councillors and staff must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but Councillors and staff are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and Safety

1. Councillors and staff who work in council offices will be provided with an appropriate workstation.
2. The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment.
3. Any staff member who feels that their workstation requires changes to make it compliant must speak to the Clerk. Annual display screen equipment risk assessments are completed by every member of staff who regularly uses this equipment.

Password and Authentication

All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

To further strengthen account security:

- Initial user account passwords will be generated by the Clerk's Office and theses must be changed immediately.
- Service or System (e.g. Website) account passwords are generated and managed by the Clerk's Office.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

1. Access to Passwords
    - Passwords are personal and must not be shared under any circumstances.
    - Only the assigned user of an account may access or use the associated password.
    - In exceptional cases (e.g., incident response, Freedom of Information requests, or employee offboarding), access to system credentials may be granted to the Clerk's Office, with appropriate approvals and logging.
    - Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Town Clerk, in a sealed envelope, only to be accessed in an emergency.
2. Password Storage and Management
    - Passwords must not be stored in plain text or written down in insecure locations.
    - Passwords must be stored using a council-approved, encrypted password manager.
3. Password Change Requirements
    - Immediately change your password if compromise is suspected.
4. Responsibility
    - Users are responsible for creating and maintaining secure passwords for their accounts.

Monitoring

The Council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

1. The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.
2. Monitoring of a councillors or staff member's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.
3. The information obtained through monitoring may be shared internally, including with councillors and staff if access to the data is necessary. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.
4. The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

5. Councillors and staff have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.
6. Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.
7. The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.
8. Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.
9. All computers will be periodically checked and scanned for unauthorised programmes and viruses.

Remote Working

Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home or at any other external premises), as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the device does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;
- the location and direction of the screen should be checked to ensure confidential information is out of view. Sufficient steps should be taken to avoid messages being read by other people.
- any data printed should be collected and stored securely;
- if using a personal device, all electronic files should be password protected and the data saved to the council's system/services when accessible. Once the data has been uploaded to the council's system, it should then be deleted from the personal device.
- papers, files or computer equipment must not be left unattended at an external premises;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;

Email Usage

Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors

and staff need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

1. On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors and staff are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.
2. These rules are designed to minimise the legal risks run when using email at work and to guide councillors and staff as to what may and may not be done. If there is something which is not covered in the policy, Councillors and staff should ask the Clerk's Office, rather than assuming they know the right answer.
3. All councillors and staff who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.
4. Should a councillor resign, their email access will be rescinded immediately. The account will be deleted from the council's system after six months.
5. Email messages sent on the council's account should be for council use only. Personal communications are permitted provided they do not encroach upon working time or interrupt council business in any way. Employees and other authorised users are asked to restrict their personal use to official lunch breaks or before or after working hours, and to use their personal email accounts, rather than council addresses.

Use of the Internet

Copyright

Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

1. It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.
2. Councillors and staff should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).
3. Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.
4. Copyright and database right law can be complicated. Councillors and staff should check with the Clerk's Office if unsure about anything.

Trademarks, links and data protection

The council does not permit the registration of any new domain names or trademarks relating to the council's names or products, unless authorised to do so.

Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy.

Accuracy of Information

One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

Use of Social Media

Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

1. Personal use of social networking/media and chat sites are not permitted during working hours.
2. The council recognises the importance of councillors and staff joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.
   However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks about could be regarded by anyone as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors and staff should be aware that parishioners or other local organisations may read their personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.
3. To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:
   - Contacts from any of the council's databases should not be downloaded and connected with any social networking sites with electronic address book facilities.
   - Care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") **Writers must not claim or give the impression that they are speaking on behalf of the council.**
   - Any employee who is developing a site or writing a blog that will mention the council must inform the Clerk's Office and gain agreement before going 'live'.
   - The council expects Councillors and staff to be respectful about the council and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.

- Comments posted by councillors and staff on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations should not take place on any social networking sites, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors and staff might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other Councillors and staff anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.
- Councillors and staff must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles (as covered in the Social Media for Councillors policy). Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other Councillors and staff can raise grievances for alleged bullying and/or harassment.
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council, its councillors or its staff, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the Clerk's Office.
- Councillors and staff who use social media sites must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors and staff who use social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor or member of staff. All such contacts will be considered council property and may be subject to disclosure upon request.

4. Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile must not misrepresent themselves or their role with the council. Councillors and staff are also advised that social media sites are not an

appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

5. It is important to note that contact details and information remain the property of the council. In addition, councillors and staff leaving the council will be required to delete all council-related data including contact details from any personal device / equipment.

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

Review

Signed:

Cllr P Davidson

Cllr Pamela Davidson

Chair, Appleby-in-Westmorland Town Council

Signed:

S Gilbertson

Sue Gilbertson

Clerk & RFO (Appleby-in-Westmorland Town Council)

Adopted by Appleby-in Westmorland Council on 24th June 2026

Review Date: June 2028