BERRYNARBOR PARISH COUNCIL

Information Technology Policy

Adopted 10 March 2026

Contents

This policy has been developed in line with the National Association of Local Councils (NALC) guidelines.

1. Purpose

The purpose of this policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. It will help to:

- 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.

2. Scope

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-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.
This

3. 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. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address.

4. Computer Use

4.1 Hardware

Council computer equipment is provided for council purposes; however reasonable personal use is permitted (reasonable interpreted as in the opinion of the Clerk). Any personal use of our computers and systems should not interrupt our daily council work in any way.

- Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work.

- All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.
- Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.
- A database of equipment issued will be kept.
- Any faults or necessary repairs must be reported to the Clerk.

4.2 Portable Equipment

Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

- It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

- All portable computers must be stored safely and securely; should not be left unattended when away from council premises and should never be left in parked vehicles.

- 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.

- Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. *NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018*.

- To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior written permission of The Clerk, This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

- 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).

5. Use of Own devices

The Council recognises that councillors, staff, and other authorised users use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the cloud, or access data in other services.

- Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated
- However, the same security precautions apply to personal devices as to the council's desktop equipment. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.
- 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).
- 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.

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. The following data must never be accessed or processed on a personal device.

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.

Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow *Western Web* to access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device. Leavers are required to confirm in writing that all Council data has been erased from devices.

Councillors, staff, and other authorised users 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, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

6. Password and Authentication Policy

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.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider, (Western Web).
- Default passwords provided by vendors or the IT provider (Western Web) must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider (Western Web).

- 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.

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

6.1 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 or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Clerk, in a sealed envelope, only to be accessed in an emergency.

6.2 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 (e.g., LastPass, Bitwarden, or KeePass).

6.3 Password Change Requirements

- Immediately change password if compromise is suspected.

6.4 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident.

6.5 Responsibility

Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider (Western Web) is responsible for:

- Managing system/service credentials.
- Enforcing password policies.
- Auditing and monitoring password-related security practices.

7. 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.

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.

Monitoring of an employee'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.

The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. 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.

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.

Councillors, staff, and other authorised users 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.

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.

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.

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.

All computers will be periodically checked and scanned for unauthorised programmes and viruses.

8. Email

Council email facilities are intended to promote effective and speedy communication on work-related matters.

These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask Western Web rather than assuming they know the right answer.

All councillors, staff, and other authorised users 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.

Email messages sent on the council’s account are for council use only. Personal use is not permitted.

9. Use of the Internet

9.1 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.

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.

Councillors, staff, and other authorised users 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).

Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Data Protection Officer if unsure about anything.

9.2 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 anywhere in the world, unless authorised to do so. Nor should they add links from any of the council’s web pages to any other external sites without checking first with the Parish Clerk.

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

9.3 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.

10. 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.

The council recognises the importance of councillors, staff, and other authorised users 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 could

be regarded 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, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' 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.

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:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of Berrynarbor Parish Council. Even if the council is not mentioned, 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, *e.g.* "our current or potential plans, councillors, staff, and other authorised users, partners"], must inform the Parish Clerk that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff, and other authorised users to be respectful about the council and its current or potential 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.
- Photos or videos, or audio recordings must not be taken on council premises without explicit permission
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with external stakeholders 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, staff, and other authorised persons, 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, staff, and other authorised users 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, staff, and other authorised users 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. 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, staff, and other authorised users 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 or councillors, staff, and other authorised users, 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 Parish Clerk.
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other 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.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff,

and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.

- 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, member of staff, or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users 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.

11. 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.

Policy will be reviewed every three years.

Date of Annual Review	Change Description	Minutes Number
10 March 2026	Policy Adopted	2603/14