CHIRTON AND CONOCK PARISH COUNCIL INFORMATION TECHNOLOGY POLICY

Introduction

Each council will have its own IT setup and, as such, a single ‘one-size-fits-all’ IT policy is unlikely to be appropriate. Some smaller parish councils may operate with minimal equipment, while others may manage multiple devices connected to a central server. These guidelines are intended to help councils identify key considerations when developing or updating their own IT policy.

Councils that use external IT providers should ensure their policies accurately reflect current practices and contractual arrangements.

Purpose of the IT Policy

The purpose of an IT 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. A well-defined policy helps 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.

Councils will also need to determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

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

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, 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

1.1 Hardware

1.1.1 If Council computer equipment is provided for council purposes, then reasonable personal use is permitted (reasonable interpreted as in the opinion of the council and the clerk.

1.1.2 Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access.

1.1.3 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.

1.1.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.1.5 Equipment should not be dismantled or reassembled without seeking advice.

1.1.6 Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software). Unless previously authorised.

1.1.7 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the council.

Equipment

2.1 Portable equipment

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

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

2.1.3 All portable computers must be stored safely and securely when not in use. Portable equipment should never be left in parked vehicles.

2.1.4 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. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

2.1.5 If an item of portable equipment is lost or damaged this should be reported to the Council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first £50 of the loss/damage.

2.1.6 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, without the prior permission of the council. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.7 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).

2.1.8 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 clerk.

2.2 Use of own devices

2.2.2 The Council recognises that some councillors, staff, and other authorised users may wish to 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 council's network or to store data on the council's server or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. 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.

2.2.3 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.

2.2.4 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). For Workers or Contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

2.2.5 In cases of legal proceedings against the council or the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

2.2.6 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.

2.2.7 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a strong password to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 5 of failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 20 minutes;
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email);
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.8 Personal data relating to the council 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. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.2.9 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.

2.2.10 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.

2.2.11 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.

2.2.12 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.

2.2.13 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 an officer access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.14 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.

Health and safety

3.1.1 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.

Password and Authentication Policy

4.1.1 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:

- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- 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

4.1.2 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.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

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

4.1.6 Responsibility

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

Monitoring

5.1.1 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.

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

Remote working

6.1.1 Increased IT security measures apply to those who work from home 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 devise 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. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- all electronic files should be password protected and the data saved to the council's system/services when accessible;
- any data should be kept safely and should only be disposed of securely;
- 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;

6.1.2 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

Email

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

7.1.2 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, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email 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 the clerk, rather than assuming they know the right answer.

7.1.4 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.

7.1.5 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.

Use of the Internet

8.1 Copyright

8.1.1 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.

8.1.2 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.

8.1.3 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).

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

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

8.2 Trademarks, links and data protection

8.2.1 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 clerk.

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

8.3 Accuracy of information

8.3.1 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.

9 Use of social media

9.1.1 Use of Official Accounts

The Parish Council operates a Facebook account for the promotion of activities and events and as a communication and broadcast tool.

- Examples of acceptable corporate content are:
- Marketing campaigns
- Consultation documents
- News feed & emergency information
- Event listings
- Key dates
- Short debates & quick comments on hot topics and relevant news (discussion board)
- Polls and information gathering
- Useful links

9.1.2 The following outlines the limits of their use: An official account on any social media website that purports to represent the Parish Council may only be set-up with consent from the Parish Council. Once approved, each account will be set up by the Parish Clerk or Chairperson or other nominated, responsible officer. Only authorised persons may use these accounts to post online and access to the account is strictly

limited. The Parish Council's social media accounts are managed and monitored daily by the Parish Clerk and Chairperson they are allowed to post links to the corporate website, partner websites, 'Useful' links for example local transport sites etc, links to other Facebook pages, local media e.g. National organisations . confidentiality policy and data protection policy. Social media accounts will primarily be used to promote the 'good news' and information, supplementing content already published on the Parish Council's website. Any employee, Councillor or member of the public who becomes aware of social networking activity that would be deemed distasteful should make the Parish Clerk and/or the account administrator aware as soon as possible

9.1.3 Facebook

The Parish Council's Facebook page. Facebook pages are used to highlight news, make announcements, engage with the community and share information. Comments posted on and messages received on the Facebook page are views of individuals and do not represent the views of the Parish Council.

9.1.4 Social media moderation policy

The Parish Council Facebook page is reactively moderated. The Council cannot accept responsibility for the content of any comment by a third party.

- The Council reserve the right to remove comments received on Facebook that:

- Contain abusive, obscene, indecent or offensive language, or link to obscene or offensive material
- Contain swear words or other sorts of profanity
- Are completely removed from the topic of conversation or are not relevant to the item posted on the wall
- Contain abusive language towards an individual involved in the thread, other organisations or the page administrator
- Constitute spam or promote or advertise products, except where it is for an event, publication or similar item that has direct relevance to the subject of discussion. Information about locating and sharing knowledge and expertise is welcomed, but within the specific discussion
- Are designed to cause nuisance to the page administrator or other users

For serious and/or persistent breaches of the moderation policy, we reserve the right to prevent users from posting further comments.

9.1.5 Use of Photos and Video

Only The Parish Clerk & Chair has permission to upload photos and videos. The appropriate permissions must be obtained for all imagery.

9.1.6 Personal Accounts on Social Media

Staff and Councillors need to use social networking in a way that does not conflict with the terms of their contract of employment and/or the Code of Conduct. The absence of, or lack of, explicit reference to a specific website or service does not limit the extent of the application of this policy. Where no policy or guidelines exist, employees should use their professional judgment and take the most prudent action possible. If the Parish Council is referred to in a way that is deemed defamatory or confidential information is disclosed, it reserves the right to report the comment and request that it be removed.

Councillors are at liberty to set up accounts using any of the tools available but should ensure they are clearly identified as personal and do not in any way imply that they reflect the Council's view or are made on behalf of the Council. Councillors should at all times present a professional image and not disclose anything of a confidential nature. Comments of a derogatory, proprietary or libellous nature should not be made and care should be taken to avoid guesswork, exaggeration and colourful language.

9.1.7 Purdah

In the six week run up to an election – local, general – councils have to be very careful not to do or say anything that could be viewed in any way to support any political party or candidate. The period is known as purdah. The Council will continue to publish important service announcements using social media but will monitor and potentially have to remove responses if they are overtly party political.

9.1.8 Responding to direct messages

Social Media users requesting to send a direct message to the Parish Council via the Facebook platform are directed to contact the PC via the Clerk's email address instead. All formal requests, comments, enquiries or complaints should be emailed to the Parish Council using the email addresses and/or contact form on the website.

9.1.9 Rules The Parish Council may monitor forums and blogs to gain indirect feedback. The Parish Council may post replies on forums or blogs to answer queries or address factual corrections, but would generally take a cautious approach before getting involved in contentious issues.

The Parish Council reserves the right to take any necessary steps to protect members of the Parish community and will delete any comments referencing the Parish Council, which are deemed abusive or offensive in any way.

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.

This IT Policy was approved and adopted by Chirton & Conock Parish Council at a full Parish Council Meeting held on 12th May 2026.

Signed: ……..……

Chairman: P Radford - Howes