CONGLETON TOWN COUNCIL

COMMITTEE REPORTS AND UPDATES

COMMITTEE:	**Council**		
MEETING DATE AND TIME	**4th April 2024 7.00 pm**	**LOCATION**	**Congleton Town Hall**
REPORT FROM	**Serena Van Schepdael: R.F.O**		
AGENDA ITEM REPORT TITLE	**Item 7 ICT Policy Review**		
Background	The ICT Policy was requested to be reviewed after the Business Risk Assessment was approved with the addition of Cyber Security Risks. The original updated draft was rejected by the Council on 10th August 2023, one comment made during discussions was to see if NALC (National Association of Local Councils) have a template to use.		
Updates	NALC does not have a template, but they do provide guidelines for what to include in an Information Technology Policy. This draft policy is based on those guidelines. Please see the current Policy here: Congleton Town Council ICT Policy (congleton-tc.gov.uk) Each item in the NALC guidelines has been considered when drafting this policy. The sections in the current document that have been removed are Health & Safety and Protocol for using the Council's website. See Appendix 7.1 for the new DRAFT ICT and Cyber Security Policy which was approved by the Finance & Policy Committee on 14th March 2024. It was requested that this document be reviewed every 2 years, and at the next review consider adding AI protection/information into the policy.		
Financial	No requirements/implications for this decision.		
Environmental	No implications for this decision.		
Equality and Diversity	No implications for this decision.		
Decision Request	To approve the updated ICT Policy and adopt into the Constitution.		

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

[ENTER COUNCIL NAME] INFORMATION TECHNOLOGY POLICY GUIDELINES

Each council will have their own IT provision and a 'fit-for-all' policy is not possible. Some small Parish councils will have minimal equipment whilst others may multiple devices linked to a server. These guidelines are designed to help councils consider some of the factors that may need to go into a policy. Those councils with external IT providers should ensure any policy reflects the current practice.

The purpose of an IT policy is to set out the parameters on how council staff should use the technology that you provide them with in order to do their job.

A clear policy will also help to raise awareness of the risks associated with using IT and can protect the council from loss of data. Councils will need to take a view on whether staff are permitted to use IT equipment for personal use (i.e. accessing webmail or online shopping at lunchtimes). The policy needs to clarify acceptable and non-acceptable use and what will happen if the policy is breached.

As an employer you have the right to monitor work use of IT equipment provided you have a legitimate reason and that you tell staff that you might do this.

When drafting your IT Policy, use the following questions/points to guide the areas to cover:

1. Who does the policy apply to?
2. What communications and IT equipment does the policy cover? For example, computers, internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones etc.
3. Who is responsible for monitoring and reviewing the policy? Ideally there should be one individual with overall responsibility. This person should help staff understand the policy and enforce it.
4. Related policies – what other policies do you have which set out standards of behaviour that apply equally to online behaviour? Examples may include Disciplinary Rules, Data Protection Policy, Equality and Diversity Policy etc.
5. Monitoring – Do you monitor how staff use the internet, email or work telephones? Employers are able to do so in particular circumstances although this would need to be properly communicated in the policy. If you have CCTV then you will need a separate policy to explain how you store and use the records. If you allow staff to use equipment for personal use, staff should be made aware that you may still monitor usage.
6. Passwords – What are your rules around passwords and accessing IT systems? Can they be disclosed? If so, to whom? What happens if you need to access another

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

employees' computer system (for example if they are off sick)? Do you transmit confidential or personal sensitive information and if so, what are your password protection protocols? What length and form must passwords be? What should an employee do if they think someone else knows their password? If password protected documents are emailed, how should the password be notified?

7. Computer usage – clarify that computers should be shut down at the end of every day. Should employees log out of their systems when they move away from their desks? Should documents be saved in a location accessible for back up? What precautions are needed for areas with public access?
8. Do you allow individuals to bring in their own IT equipment and use then for work purposes? If you do, are there restrictions or specific requirements?
9. Data Protection – ensure you reference the requirements when processing personal data in accordance with the six data protection principles. Your policy should explain your rules on collecting, storing, retaining, using disclosing and disposing of personal information. It should also set out how the council protects data and prevents unauthorised or unlawful processing or disclosure.
10. Mobile phone texting – is this appropriate for work issues? Who to (members of the public, suppliers, LA's etc)? Should abbreviations be avoided? Text messages from the council are treated in the same way as emails, for example they must not contain illegal or discriminatory content.
11. Email: What rules do you need to consider with regard to email communication? Email is sometimes seen as a casual way to communicate and this may present a reputational risk. Clear rules on email may also prevent staff from inadvertently entering into an agreement with a supplier.
12. Internet – what can the internet at work be used for and what can't it be used for? Is a firewall in place? What does this mean for staff? What limits are there on accessing chat rooms, messaging services, blogs etc from work IT and communication systems?
13. Software – what rules and controls are in place for downloading software onto work machines.
14. Training – consider including a few words on what training and support exists for staff with regards to information security. For example, do you train staff as part of their induction on the risks of email security?
15. Misuse – be clear that misuse of IT facilities can potentially result in disciplinary proceedings. What constitutes misuse? Examples could include not adhering to the policy; attempting to discover a user's password; using the computer systems to act abusively; attempting to circumvent the network's security; knowingly running and installing programmes intended to damage the computer systems; deliberately wasting computer resources; leaving laptops unattended in a public place etc.

Guidance

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

Where there is text in [square brackets] this part may be updated or be deleted if not relevant. An alternative option may have been provided.

Important notice

This is an example of an employment policy designed for a small council adhering to statutory minimum requirements and does not constitute legal advice. As with all policies it should be consistent with your terms and conditions of employment.

This document was commissioned by the National Association of Local Councils (NALC) in 2019 for the purpose of its member councils and county associations. Every effort has been made to ensure that the contents of this document are correct at time of publication. NALC cannot accept responsibility for errors, omissions and changes to information subsequent to publication.

This document has been written by the HR Services Partnership – a company that provides HR advice and guidance to town and parish councils. Please contact them on 01403 240 205 for information about their services.

CONGLETON TOWN COUNCIL

ICT AND CYBER SECURITY POLICY

Introduction

- Congleton Town Council has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.
- The Chief Officer is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.
- Line managers have a responsibility to ensure that staff they supervise comply with this policy.
- The Council has a duty laid down in the Data Protection Act 2018, to ensure the proper security and privacy of its computer systems and data. All users have, to varying degrees, some responsibility for protecting these assets. Users also have a personal responsibility for ensuring that they and, where appropriate, the staff they supervise or have control over, comply fully with this policy – See also the Council's Information and Data Protection Policy.

1. Who does the policy apply to/ General Principles

- All staff and Councillors and volunteers using CTC equipment.
- All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Chief Officer. As a general rule, users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.
- All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection & Retention Policy'.
- All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Chief Officer.
- All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.
- All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Chief Officer.

2. What communications, IT equipment and other areas does the policy cover

- Computers and Laptops
- Remote Access Connections
- Mobile Phones and Tablets

- Emails and Email Servers
- Portable Devices
- Internet Access
- Website and Social Media
- Passwords
- Viruses
- Software
- Cyber Security
- Training

3. Who is responsible for monitoring and reviewing the policy?

- CO Reviewing
- Line Management for Monitoring of staff.

4. Related policies

- Data Protection Policy
- Social Media Policy
- Equality and Inclusion Policy

5. Passwords and Password Protection

All council computers and systems must be password protected to prevent unauthorised access.

- Where possible, two factor authentication should be utilised.
- Users should ensure that unattended devices are password protected.
- Where users have unique access permissions and/or accounts for systems, these must not be shared with other users.
- Different passwords should be used for different devices and accounts.
- Passwords should be routinely changed.
- Passwords should not be written down or left in unsecure locations.
- Passwords must not be inserted into email messages or any other form of communication, or saved onto a shared computer.
- Additional Information:
    - The National Cyber Security Centre Website provides information on passwords.

6.Training

Employees and Councillors should be provided with regular cybersecurity training as is appropriate for their role and level of systems access.

7.Misuse of I.T

Misuse includes, but is not limited to:

- Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material.
- Creation of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety.
- Creation or transmission of defamatory material
- Transmission of material which in anyway infringes the copyright of another person.
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
    - i. Wasting staff effort or networked resources
    - ii. Corrupting or destroying another users' data.
    - iii. Violating the privacy of other users.
    - iv. Disrupting the work of other users.

- Other misuse of the networked resources by the deliberate introduction of viruses/malware
- Playing games during working hours
- Altering the set up or operating perimeters of any computer equipment without authority.
- Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited.
- Any personal IT equipment must not be connected to any Council IT equipment.

8.Security and Virus Controls

- Consideration must be given to the secure location of equipment and documentation to help safeguard the Council's ICT assets. Portable equipment must be locked away when not in use and must not be removed from the premises without permission.

- Only persons authorised by the Chief Officer may use Council computer systems. The authority given to use a system must be sufficient but not excessive and users must be notified that the authority given to them must not be exceeded.

- Operating procedures are required to control use of ICT equipment.

- Security incidents relating to any aspect of this policy must be reported to the Chief Officer immediately.

- Avoid using public wi-fi connections that are not secure.

Virus Controls

- Viruses are undesirable pieces of computer code that can corrupt systems, equipment, and data. They are a serious, increasing threat to the computer systems of the Council.

- If a virus is suspected, the equipment should be switched off and isolated and the Council's support contractor should be contacted.

- Viruses are easily transmitted via email and internet downloads. In particular, users must:
    - not transmit by email any file attachment which they know to be infected with a virus.
    - not download data or programs of any nature from unknown sources
    - not forward virus warning
    - contact the Councils IT providers of any scam emails that arrive.

- All computer and servers will have loaded and operate the Council's standard virus detection software for scanning.
- No software should be located onto the Council's equipment without the permission of the Chief Officer.

9. Computer use

- Laptops and Computers must be shut down at the end of every day and kept in a secure locked cabinet.
- Laptops and Computers must be logged out when member of staff is away from their desk.
- For computers in public areas, these must be secure and out of reach of the public and logged out when away from desk.

10. Use of E-mail

E-mails sent or received form part of official records of the Council, they are not private property. E-mails may be disclosed under the Freedom of Information Act, as part of legal proceedings (e.g. tribunals) and as part of disciplinary proceedings.
Employees are responsible for all actions relating to their e-mail accounts/username and must ensure that no other person has access to their account without the permission or knowledge of the Chief Officer or Deputy Chief Officer.
When using the Council's e-mail employees **must**:-

- Correctly maintain their own e-mail folders and delete all unwanted mail on a regular basis.
- Not use e-mail for the creation, retention, or distribution of disruptive or offensive messages, images, materials, or software that includes offensive or abusive comments about ethnicity, nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs, or social background. Employees who receive e-mails with this content must report the matter to their line manager.

- Not send e-mail messages that might be considered by the recipients as bullying, harassing, abusive, malicious, discriminatory, defamatory a d libellous or containing illegal or offensive material or foul language
- Not upload, download, use, retain, distribute, or disseminate any images text materials or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- Not engage in any activity that is outside the scope of normal work related duties.
- Not send chain-letters of joke e-mails
- Personal use of the Council's e-mail is NOT permitted without the prior permission of your line manager and should be restricted to the employees break periods if permitted.

11. Use of the Internet

Use of the internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of the Council in mind reasonable personal use is permissible, but this is to be restricted to break periods.
Employees **must not**:-

- Participate in any on-line activity that would bring the Council into disrepute.
- Visit, view, or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography) obscene matter, race hate material, gambling, and illegal drugs.
- Knowingly introduce any form of computer virus into the Council's computer network
- Download commercial software or any copyright material belonging to third parties unless agreed.
- Use the internet for personal financial gain.
- Use gambling or on-line auction sites or social networking sites, unless it is for the purpose of carrying out their duties, such as Facebook/Twitter for marketing.
- Abuse of these procedures could lead to disciplinary action being taken.

12.Cyber Security

Implementing effective ICT security measures is a key part of safety controls and risk management of running the Council. Following the ICT Policy procedures will help to keep awareness of cyber security and protection.

- Training and awareness course should be made available to all Staff and Councillors.
- Current and up to date information should be shared with all Staff and Councillors.
- Cyber Security must be included as part of the Councils Risk Management Policy.

Additional Information
National Cyber Security Centre: Toolkit for Public Bodies:

- https://www.ncsc.gov.uk/section/information-for/public-sector
- https://www.ncsc.gov.uk/collection/board-toolkit/toolkits-toolbox