IT SECURITY POLICY

For Employees & Councillors

Of Camelford Town Council

Adopted 17 July 2018

Contents

Introduction

Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

This IT security policy helps Camelford Town Council (CTC) to:

- Meet our legal obligations under the General Data Protection Regulation and other laws
- Reduce the risk of IT problems
- Plan for problems and deal with them when they happen
- Keep working if something does go wrong
- Protect Council and employee data
- Keep valuable Council information

Responsibilities

- Town Clerk is responsibility for the IT security strategy
- Deputy Town Clerk has operational responsibility for implementing this policy
- Andy Lawler, Yetiserve is the IT partner organisation CTC use to help with our IT support
- Seadog IT – website support
- Town Clerk is the Data Protection Officer to advise on data protection laws and best practices

Review Process

CTC will review this policy annually.

Information Asset Classification

CTC will only classify information assets which are necessary for the completion of our duties. CTC will also limit access to personal data to only those that need it for processing. In most cases, this will be the Clerk and Deputy Town Clerk.

Information Asset	**Classification**
Employee information (name, address, contact numbers, pay, sick records etc)	Employee Confidential
Councillor information (name, address, contact numbers)	Unclassified (information is public)
Council confidential (Part 2 paperwork – e.g. quotes, tenders, Code of Conduct investigations)	Council Confidential
Allotment tenant information (name, address and contact numbers)	Resident Confidential

The deliberate or accidental disclosure of any confidential information has the potential to harm the Council. This policy is designed to minimise the risk.

Access Controls

Internally, as far as possible, CTC operate on a "need to share" rather than a "need to know" basis with respect to Council confidential information. This means that our bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.

CTC operate in compliance with the GDPR "Right to Access". This is the right of data subjects to obtain confirmation as to whether CTC are processing their data, where CTC are processing it, and for what purpose. Further, CTC shall provide, upon request, a copy of their personal data, free of charge in an electronic format.

The office of the Town Clerk and Deputy Town Clerk is secured by a door entry system. The code is only known by the Town Clerk, Deputy Town Clerk, the Library Administrator and Andy Lawler (Yetiserve).

Physical files are stored within the office of the Town Clerk and Deputy Town Clerk, and this door is also secured by a door entry system. The code is only known by the Town Clerk, Deputy Town Clerk, the Library Administrator and Andy Lawler (Yetiserve).

To protect confidential information, CTC implement the following access controls:

Employee Confidential	Town Clerk Deputy Town Clerk	Password protected computers "Staffing folder" on network has security restrictions
Council Confidential	Town Clerk Deputy Town Clerk Mayor	Password protected computers
Resident Confidential (Allotment tenants)	Deputy Town Clerk	Password protected computer

In addition to the above, the Library Administrator will be given limited access to files in order to carry out duties in the absence of the Deputy Town Clerk.

Security Software

To protect our data, system and users, CTC use the following systems:

Laptop and desktop anti-malware/firewall (AVG Antivirus)

Our website is hosted on servers in the UK at a secure data centre within a secure compound with razor-wire fences, 24hr security personnel, CCTC throughout and 24/7 technicians on site. Our server is kept separate from everyone else. Web Application Firewall (WAF) is always on, protecting our website with our application-specific security shield to help guard against exploits. In addition, we have installed a premium WordPress plugin that provides a wide range of security features such as:

- Brute Force Attach prevention to lock out any attempts to brute-force guess our WordPress password
- Real Time Threat defence feed – protection from the latest threats, delivered as they emerge. This provides our Firewall and Scan Engine with updated firewall rules, the latest malware signature, malicious IP updates.

- Malware Scanner – Scan for Malware, Bad URLs, Backdoors and DNS changes.

Where Information is Stored

All documents used by the Clerk and Deputy Clerk are stored on: Network/Clerk/Public Documents. The Clerk and Deputy Clerk have access to all files. Other staff have access to all files except Staffing, which has a security filter. Each computer is password protected.

Email

The Council currently use Outlook 2016. CTC are in the process of moving all Councillors to a "Camelford-tc.gov.uk" email by August 2018. This is in line with GDPR requirements.

Currently, our email is a legacy version of Gmail as part of the GSuite package from Google. Google security features include Gmail spam protection which filters out suspicious emails, Gmail encryption which keeps emails private and Gmail also supports encrypted connections, which makes it harder for unauthorised persons to read what we are sending. Gmail also warns about possible security risks.

Before forwarding any emails, you should inform the originator to whom you intend to forward the email and for what purpose. If the email has been sent by a resident who would like to have the email included in correspondence at the next meeting, you should inform the resident that the email will be sent to all Councillors and will be in the public domain. The email address will be redacted and the sender should be advised of this.

Should any member of staff or Councillor receive a suspicious email, they should advise the Town Clerk immediately and are advised not to open the email or attachments.

Employees/Councillors Joining and Leaving

When a new employee joins CTC, CTC will add them to our secure email system. Town Clerk and Deputy Town clerk roles will also have full access to the Public Documents files. New Councillors will be added to our secure email system.

CTC will provide training to new employees and support for existing staff to implement this policy. This includes an initial introduction to IT security, covering the risks, basic security measures, CTC policies and where to get help.

Employee and Councillor responsibilities

Effective security is a team effort requiring the participation and support of every employee and Councillor. It is the responsibility of employees and Councillors to know and follow these guidelines.

Individuals are personally responsible for the secure handling of confidential information that is entrusted to them. They may access, use or share confidential information (e.g. Part 2 paperwork, personal information) only to the extent it is authorised and necessary for the proper performance of their duties. Individuals are responsible for prompt reporting of any theft, loss, unauthorised disclosure of protected information or any breach of this policy to the Town Clerk.

Protecting your own device(s)

It is also your responsibility to use your personal devices (computer, phone tablet etc.) in a secure way. However, CTC will provide training and support to enable you to do so (see below). At a minimum:

- Remove software that you do not use or need from your computer.
- Update your operating system and applications regularly.
- Keep your computer firewall/antivirus switched on.
- Store files in Council storage locations (Public documents) so that is backed up properly and available in an emergency. For those Councillors using personal computers/laptops, CTC advise that you password protect your Council correspondence.
- Understand the privacy and security settings on your phone and social media accounts.
- Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work separate from any family or shared computers.
- Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in.
- If you need to go away from your desk, log out.

Public Wifi

A public Wi-Fi does not necessarily provide a secure connection to the internet. Risks include:

Man in the Middle attacks

One of the most common threats on these networks is called a Man in the Middle (MitM) attack. Essentially, a MitM attack is a form of eavesdropping. When a computer makes a connection to the Internet, data is sent from point A (computer) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and "read" them. So what you thought was private no longer is.

Unencrypted networks

Encryption means that the messages that are sent between your computer and the wireless router are in the form of a "secret code," so that they cannot be read by anyone who doesn't have the key to decipher the code. Most routers are shipped from the factory with encryption turned off by default, and it must be turned on when the network is set up. If an IT professional sets up the network, then chances are good that encryption has been enabled. However, there is no surefire way to tell if this has happened.

Malware distribution

Thanks to software vulnerabilities, there are also ways that attackers can slip malware onto your computer without you even knowing. A software vulnerability is a security hole or weakness found in an operating system or software program. Hackers can exploit this weakness by writing code to target a specific vulnerability, and then inject the malware onto your device.

Snooping and sniffing

Wi-Fi snooping and sniffing is what it sounds like. Cybercriminals can buy special software kits and even devices to help assist them with eavesdropping on Wi-Fi signals. This technique can allow the attackers to access everything that you are doing online — from viewing whole webpages you have visited (including any information you may have filled out while visiting that webpage) to being able to capture your login credentials, and even being able to hijack your accounts.

Malicious hotspots

These "rogue access points" trick victims into connecting to what they think is a legitimate network because the name sounds reputable. Say you're staying at the Camelford Inn and want to connect to

the hotel's Wi-Fi. You may think you're selecting the correct one when you click on "Cam Inn," but you haven't. Instead, you've just connected to a rogue hotspot set up by cybercriminals who can now view your sensitive information.

How to stay safe on public Wi-Fi

The best way to know your information is safe while using public Wi-Fi is to use a virtual private network (VPN), like Norton WiFi Privacy, when surfing on your PC, Mac, smartphone or tablet. However, if you must use public Wi-Fi, follow these tips to protect your information.

Don't:

- Allow your Wi-Fi to auto-connect to networks
- Log into any account via an app that contains sensitive information. Go to the website instead and verify they are using HTTPS before logging in
- Leave your Wi-Fi or Bluetooth on if you are not using them
- Access websites that hold your sensitive information, such as such as financial or healthcare accounts
- Log onto a network that isn't password protected

Do:

- Disable file sharing
- Only visit sites using HTTPS
- Log out of accounts when done using them
- Use a VPN, like Norton WiFi Privacy, to make sure your public Wi-Fi connections are made private

Camelford Town Council/Cornwall Council Wifi

CTC have wifi which is secured, as well as Cornwall Council wifi for library users. These are both secure and regularly tested.

Password Guidelines

- Change default passwords on computers, phones and all network devices regularly
- Don't share your password with other people.
- Don't write down passwords next to computers and phones
- Use strong passwords
- Don't use the same password for multiple critical systems

Be Alert to other security risks

- While technology can prevent many security incidents, your actions and habits are also important.
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender.
- Be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information, including employee or Council confidential information.
- Be wary of fake websites and phishing emails. Don't click on links in emails or social media.
- Use social media, including personal blogs, in a professional and responsible way, without violating Council policies or disclosing confidential information.

- Take particular care of your computer and mobile devices when you are away from home or out of the office.
- If you leave the Council, you will return any Council property, and delete all confidential information from your computer as soon as is practicable. Your email address will automatically be deleted.
- Where confidential information is stored on paper, it should be kept in a secure place where unauthorised people cannot see it and shredded or put in the confidential waste when no longer required.

Backup, disaster recovery and continuity

Backups are performed live; so, each time a document is edited and saved, it is automatically backed up. Backups are stored on a Raid ARAY NAS Drive Box . This has two drives in case one fails, as an extra security measure.

In the event of an office system recovery needed, you should contact either the Town Clerk or Deputy Clerk who will contact Yetiserve immediately. For library systems, you should contact Cornwall Council.

Under the GDPR, where a data breach is likely to result in a "risk for the rights and freedoms of individuals" CTC must notify the persons affected and the Town Clerk "without undue delay". CTC will ensure any breach is reported to the Information Commissioners Office (ICO) within 72 hours.

Inventory of Hardware and Software Used

- 2 x HP 20-C010na 19.5 All in one computers
- Office 365 (outlook 2016)
- Windows 7
- Windows Defender Firewall
- AVG Antivirus
- Rialtus Software (accounts)
- Flash drive
- Laptop ASUS