Acceptable Use Policy

Author : **Michael Sage**

Date Prepared : **Oct 2023**

Version	Date	Update
0.1	23/04/2021	Initial Document (early draft)
0.2	26/04/2021	Updated from feedback
0.3	05/05/2021	Some sections reworded
0.4	08/11/2021	Further updates and clarification
0.5	18/10/2023	Included list of old policies in appendix. Added in additional wording around BYOD and device support.
0.6	29/10/2024	Added wording for using personal peripherals
0.7	12/11/2024	Added clarification for working abroad.

Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of all Chelmsford City Council's (CCC from hereafter) information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all CCC's employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Chelmsford City Council (and associated organisations) business activities worldwide, and to all information handled by CCC relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by CCC or on its behalf, including Software as a Service (SaaS) and other offsite hosted "cloud" solutions.

Computer Access Control – Individual's Responsibility

Access to the CCC IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Council's IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any CCC IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access CCC IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to CCC IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Must take extra care when using a personal (BYOD) device to access CCC network or IT systems and keep these devices up to date and run current anti-virus, applications on these systems may be monitored by CCC to ensure that the device is compliant. Any devices that no longer have manufacturer support (this includes operating systems, applications and antivirus), must not connect to CCC networks.
- CCC IT staff will never look at any personal data (nor do they have access to private data) or applications on a non-Council owned device, this means CCC Digital Services staff are unable to offer "personalised" support on a BYOD device. Limited system monitoring may occur in Office 365 on personal devices, i.e. teams, CCC email, etc.
- Store CCC data on any non-authorised equipment.
- Give or transfer CCC data or software to any person or organisation outside CCC without the appropriate checks and balances being in place.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of CCC internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to CCC in any way, not in breach of any term and condition of employment and does not place the individual or CCC in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which CCC considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble on any CCC device.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to CCC, alter any information about it, or express any opinion about CCC, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward CCC mail to personal (non-CCC) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of CCC unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download any software from the internet without prior approval of Digital Services.
- Use CCC mobile devices to access any content or incur charges that are not related directly to the job being done (i.e. gambling sites, pornography, etc)
- If using a CCC device and connecting to any internet connection outside of the Council's buildings, then the VPN must be connected and used to protect CCC data.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, CCC enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided, for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers, photocopiers or in sight on desks and should be locked away every night.

- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with CCC remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling, unless explicitly for business travel, CCC equipment must not be used abroad as geo restrictions are in place to protect the authority from nation state hackers and technical exceptions will need to be made, this must have director sign off.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.
- All devices and accessories (including loan devices) should be treated with respect. They should be stored and used in a smoke free environment and kept away from food, drink, pets and children. Any damage caused by the devices not being used and stored correctly will be charged to services who may recover the costs from the individual concerned.
- Loss of devices must be reported to Digital Services as soon as possible to enable device wipe / loss and reporting.

If you are working abroad, please make sure you pay special attention to the following:

- You will need director sign off to work outside of the UK
- Digital Services automatically lock down both the device and user if a suspicious login is detected abroad, and service managers are notified.
- If you intend to work abroad for more than 3 months a year, please contact digital services before moving, as special provision needs to be made.
- Digital Services must be informed before taking a CCC mobile abroad as it will need to have roaming activated.

- When accessing CCC Microsoft 365 applications on your personal device while abroad:
    - Data privacy and cyber security laws vary internationally - adhere to local laws and regulations.
    - Be mindful of potential data security risks, especially when using public or unsecured networks (e.g. hotel Wi-Fi).
    - Only access essential data and applications to minimise exposure of sensitive information.
    - CCC are not responsible for any foreign data / voice costs on personal devices

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only CCC authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorised by Digital Services on CCC computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on CCC computers must be approved and installed by Digital Services, we will not install personally licensed software on to corporate devices.

Individuals must not:

- Store personal files such as music, video, photographs, or games on CCC IT equipment.

Viruses

Digital Services has implemented centralised, automated, virus detection and virus software updates within CCC. All devices have antivirus software installed to detect and remove any virus automatically. Viruses and threats (and suspected viruses / threats) should be reported to the Digital Services Service Desk or CCTV out of hours as soon as possible.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved CCC anti-virus software and procedures.

Use of Personal Peripherals (i.e. keyboards, mice)

Individuals are permitted to connect personal peripherals (keyboards, mice and headphones only) to CCC devices in CCC offices or at home. In addition staff may connect additional monitors to CCC devices at home in line with CCCs Display Screen Equipment Procedure.

Personal peripherals must be selected from CCCs approved list of recommended peripherals to ensure compatibility and security;

This list will be published on Digitals Intranet pages and reviewed and updated when required.

Digital Services will not provide technical support for any personal equipment, including installation, troubleshooting, or maintenance.
Individuals must not:

- Damage CCC equipment by using personal equipment
- Need to install drivers to support any personal equipment

- Claim for any equipment for working from home
- Breach any HSE or Occupational Health guidelines and should always follow the correct processes if extra equipment is needed.

Digital Services can request the removal of any personal peripherals at any time, *if* they are deemed to negatively affect performance or security.

Telephony (Voice) Equipment Conditions of Use (including Microsoft Teams / Skype and mobile devices (including feature and smart phones))

Use of CCC voice equipment is intended for business use. Individuals must not use CCC voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances.

All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Voice calls and instant messages are subject to a retention policy, so all communication must be treated as if it is being recorded and subject to freedom of information (FoI) and Subject Access Requests (SAR) that are addressed to the authority.

If a device is used to take a photography or video recording, this should be uploaded to OneDrive or SharePoint as soon as possible and deleted from the mobile device as soon as possible.

Individuals must not:

- Use CCC voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators unless it is for business use.
- Use their phone when driving, unless absolutely necessary when a hands free kit must be used (the council does not encourage the use of mobiles while driving in any circumstance).

Actions upon Termination of Contract

All CCC equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Digital Services at termination of contract.

All CCC data or intellectual property developed or gained during the period of employment remains the property of CCC and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on CCC devices is the property of CCC and there is no official provision for individual data privacy, however wherever possible CCC will avoid opening personal emails (within the Council's email system).

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. CCC has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.
This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 2018

It is your responsibility to report suspected breaches of security policy without delay to your line management, Digital Services, the Information Security department or the Service Desk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Council's disciplinary procedures.

Digital Services can be reached via email, web, teams or phone:

Intranet: Welcome to Digital Services (sharepoint.com)
Email: digitalservices@chelmsford.gov.uk
Web: Self Service Portal
Teams: Digital Services CQ
Phone: +441245 606666
Out of Hours: +441245 606299

Appendix 1 – Replaced Policies

This AUP replaces the following policies:

- Removeable Media Policy
- Remote Working Policy
- Password & Authentication Policy
- IT Equipment Acceptable Use Policy
- Internet Acceptable Use Policy
- Email Acceptable Use Policy
- Clear Screen-Clear Desk Policy
- Change management Policy
- BYOD Policy