Colchester
City Council

Acceptable Use Policy

November 2024

www.colchester.gov.uk

Acceptable Use Policy

CONTEXT

We must act appropriately with the information we obtain and hold, and with the systems we use and access. How our systems, devices, telephony, email and intranet is used is important for our reputation and the trust of our customers. This Acceptable Usage Policy covers the security and use of all IT equipment. This policy applies to all employees, Councillors, voluntary workers, agency staff and contractors.

APPLICATION OF POLICY

Everyone who uses information and communications technology provided by Colchester City Council (CCC) must be aware of these policy statements and the obligations it places upon them.

Colchester City Council commits to informing all employees, members, voluntary workers, agency staff, contractors, Councillors and other third parties of their obligations. Other organisations, and their users, granted access to technology managed by the Colchester City Council must abide by this policy.

It is the responsibility of all employees to ensure that access to systems, the Council's network, and documents are secured. Passwords must be kept safe and personal to the specific user. In addition, we all have a responsibility to ensure that devices and applications are used appropriately and that the behaviour of any persons use of ICT solutions does not call the Council into disrepute. These measures should be upheld regardless of work location.

ACCESS TO IT SYSTEMS

- You must not leave user accounts logged in at an unattended and unlocked computer.
- You must not attempt to access data or systems that you are not authorised to use or access.
- You must not install, access, or modify applications, systems or data without authorisation.
- You must maintain the security of information as defined in the Information Security and Data Protection Policies.
- You must not access other people's email without their permission.
- You must not forward CCC emails to personal email accounts, which contain sensitive and/or personal data.
- If you receive or view email or other content not intended for you, you must protect its confidentiality.
- You must take care when replying or forwarding emails to ensure that only authorised individuals are included and any history in the chain or attachments are suitable to share with that individual(s).

PASSWORDS

- You must not allow anyone else to use your user username and password for any IT system.

- You must not disclose your password to anyone or ask anyone else for their password. If you suspect your password has become known to anyone else, change it immediately and report it to the ICT team.
- You must not use someone else's username and password to access any IT systems.
- You must not leave your password unprotected (for example writing it down or sharing it with another person).
- Passwords must meet the requirements of the Council's Password Policy.
- All CCC devices must be password protected (or alternately protected by other appropriate ICT approved means such as Fingerprint and PIN).

BEHAVIOUR

- You must not participate in unlawful, libellous, immoral, or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, material of a pornographic, sexual, violent, criminal, racist, sexist, or otherwise discriminatory nature. Further, you must not use the systems to perpetrate any form of fraud or piracy.
- You must not publish a website, or any content on a website, that could bring the Council into disrepute. This includes publishing defamatory or knowingly false material about the organisation, colleagues, or customers in any online publishing format.
- When representing the Council only subscribe to services with your Colchester City Council email address.
- Colchester City Council facilities and identity must not be used for commercial purposes outside the authority or remit of the Council, or for personal financial gain.
- You must not use the internet or email to make personal gains or conduct a personal business.
- You must not use the internet or email to gamble.
- You must not bring the Council into disrepute through use of online 'social networking' activities.
- You must report faults with information and communications technology to the ICT team and co-operate with fault diagnosis and resolution.
- If you use CCC technology or CCC internet provision for personal use, the Council takes no responsibility for the security of your personal information. It is recommended you do not carry out personal financial transactions.

DEVICES

- You must not connect any non-authorised device to your CCC computer, the corporate network, or corporate IT systems.
- You must not store data on any non-authorised equipment.
- In order to comply with Data Protection legislation, all Council communications must only be made using Council approved applications and devices.

STORAGE

- You must not give or transfer data or software to any person or organisation, without following the Information Security and Data Protection Policies.

- Documents must not be stored locally (for example, on C:\ drive) on a desktop computer, laptop or mobile phone, as information may be irretrievable if the device fails or is stolen. This includes synchronising SharePoint and OneDrive to a local device without ICT authorisation.
- The use of mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be authorised by the Information Services Manager. Devices will only be authorised if they can be secured through a password or similar encryption. Personal data must not be stored on mobile devices, unless approved by the Information Services Manager.

SECURITY AND LICENSING

- You must not attempt to disable or bypass anti-virus, malware, or other information security controls, and you should take care not to introduce viruses or malware. If you discover a virus or malware, you must notify ICT immediately, and disconnect the device from any network.
- You must not expose the Council to risk by clicking on links or opening suspicious attachments to phishing or scam emails.
- You must not use the email systems in a way that could affect its reliability or effectiveness, for example, distributing chain letters or spam.
- You must only use software that is appropriately licensed and materials which are not copyrighted, or for which you have been granted use.

WORKING REMOTELY

- Working away from the office must be in line with Colchester City Council's remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in clear view in a vehicle.
- Laptops must be carried as hand luggage when travelling.
- Information and equipment must be protected against loss or compromise when working remotely.
- Do not connect to untrusted/public networks such as cafes, hotels etc., as these are presumed to be more vulnerable to hacking. Tethering to a corporate mobile phone should be used in the first instance.

USE OF SHAREPOINT

- You must not purposely engage in activity that may deprive an authorised user access to a SharePoint resource.
- You must not attempt to access content for which you have no legitimate business need.
- You must not circumvent SharePoint security measures.
- All staff must maintain the supported infrastructure setup by filing documents via Adding Properties or via the Details menu and not creating folders within folders.
- Site owners are responsible for managing the use of SharePoint in their area and are accountable for their actions.
- Site owners are responsible for the custody or operation of their SharePoint sites and are responsible for proper authorisation of user access.
- Confidential or potentially sensitive data stored on SharePoint must be kept confidential and secure by the user.

- You must ensure that permissions to document libraries are appropriately set and maintained to ensure the security of information.
- Site owners should review the permissions set on their sites at least annually.
- You must ensure that private or personal documents are secured to ensure the security of information.
- Data can be shared with external people/organisations using the 'External sharing' SharePoint site where there is a justified business need. All documents shared must be removed once the need to share has expired. Any special category data shared in this way must be done with the appropriate set up of SharePoint permissions to ensure the security of that data.

USE OF ONEDRIVE

- OneDrive must not be used as a replacement for corporate shared document repository, SharePoint.
- OneDrive documents must not be kept for longer than necessary.
- If you share a OneDrive document with another user, it's your responsibility to ensure that this is done securely and appropriately and ideally only for a limited duration to permit its use.

USE OF TEAMS

- Personal data should not be shared via teams messaging.
- Where possible, work documents should be stored on SharePoint function sites, not Files tabs on Teams channels. Where it is not possible, make sure the permissions for the Teams channel are set appropriately to ensure files are only accessible by authorised users.
- All users should ensure that permissions for documents are set appropriately.
- All users should ensure that only permitted participants are added to Teams channels, chats, meeting chats and meetings.
- Care should be taken when screen sharing and/or recording a meeting to make sure that personal data is not disclosed inappropriately. Permission should be sought from all attendees before recording starts.
- Ensure that when making video calls the environment you are calling from and any backgrounds you are using are appropriate for business use.

MOBILE PHONES

- Requests for a mobile phone will be subject to a valid business case being made and management authorisation.
- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the network (please refer to the Password Policy).
- The primary reason for being given a work mobile phone is for business purposes. Using the phone for personal calls should not interfere with daily business and wherever possible be made outside of working hours.

- Employees are expected to use the internet responsibly and productively. Excessive personal internet browsing, including social media use, is not permitted.
- Mobile phones should be connected to secure wi-fi networks where available to prevent excessive use of data. Use of the mobile phone to create a hotspot to work from should be used in exceptional circumstances only. Mobile data usage will be monitored, and consistent excessive use may lead to suspension of service.
- Calls to premium rate numbers and overseas are not permitted, unless there is a real business need and authorisation has been provided by the relevant member of the Senior Leadership Team.
- You must not use Colchester City Council mobile devices for conducting private business.
- Mobile devices may not be used at any time to store or transmit illicit materials or harass others.
- When driving, staff are expected to comply with the Council's Vehicle User Handbook and the Road Vehicles (Construction and Use) (Amendment) (No4) Regulations 2003, which prohibit the use of handheld mobile devices at all times when driving.
- If your device use is deemed unacceptable, we may cancel your plan and ask for the return of the device.
- If you lose your device or it is stolen this must be reported to the ICT team without delay.

WHEN AN EMPLOYEE LEAVES

- All line managers must notify the ICT team of any leavers or changes to staff roles (permanent, temporary or casuals) so that access can be terminated or amended as appropriate.
- All IT equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the ICT team.

MONITORING

The Council maintains the right to examine any system or device used during its business, and to inspect any data held there.

To ensure compliance with this policy, the volume of internet and network traffic, and the use and content of emails and visited internet sites, may be monitored. Specific content will not be monitored unless there is suspicion of improper use.

It is the employee's responsibility to report suspected breaches of this policy without delay to their line management and to the ICT team.

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the Council's disciplinary procedures.

ICT reserve the right to withdraw a users' access to any computer systems and communication services, including internet services without notice.

POLICY REVIEW

The policy will be reviewed on an annual basis and updated as necessary at these reviews.

FURTHER INFORMATION

For further information contact ict@colchester.gov.uk

VERSION CONTROL

Purpose:	To specify how the Council maintains security
Status:	Final
Final date:	22nd November 2024
To be reviewed:	November 2025