



Colchester
City Council

Digital Systems Acceptable Use and Password Policy December 2025

www.colchester.gov.uk

Acceptable Use Policy

APPLICATION OF POLICY

All users of corporate digital devices and systems including but not limited to laptops, tablets and mobile smart phones and / or those that have access to a corporate Microsoft 365 email account / address provided by Colchester City Council (CCC), Colchester Borough Homes, Colchester Commercial Holdings Ltd. All employees, elected members, contractors, volunteers, vendors, apprentices, student/work experience placements and other partner agencies must be aware of these policy statements and are bound by the responsibilities 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, documents and data 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 person's use of Digital Team solutions does not bring the Council into disrepute. These measures should be upheld regardless of work location.

ACCESS TO DIGITAL SYSTEMS

- You must not leave user accounts logged in at an unattended and unlocked device.
- You must not attempt to access data or systems that you are not authorised to use or access.
- You must not download, install, access, or modify applications, systems or data without authorisation.
- You must maintain the security of information as defined in the Data Protection Policies.
- You must not access other people's devices or use their Microsoft 365 or application login credentials.
- You must not forward CCC emails to your own personal or work email accounts.
- You must not use any tool or rule to auto forward any email sent to your CCC account, unless part of a specific pre-defined business process, which has been pre-approved by Digital.
- If you receive or view email or other content not intended for you, you have a legal obligation to take reasonable steps to protect confidentiality contained therein.
- You must take care when replying or forwarding emails to ensure that only authorised individuals are included and any email history in the chain or attachments are suitable to share with that individual(s).
- Corporate email accounts must not be used for personal correspondence or non-Council business. All email use should be for Council-related activities, in line with the Council's Acceptable Use Policy.

- The Corporate email platform (Microsoft 365 mailboxes both individual and shared mailboxes) should not be used as file systems, important content or correspondence should be saved into SharePoint or an alternate document management system.

PASSWORDS

- You must not share or allow anyone else to use your user username and password for any Digital system.
- Password complexity requirements may change due to external risk and threat; you will change your password when requested.
- You will not write down or store your CCC Password on paper, or in any electronic device.
- You must ensure that each of your accounts uses a unique password.
- 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 Digital Team.
- You must not use someone else's username and password to access any IT systems.
- Passwords must meet the requirements of the Council's Password Policy, note, this is subject to change in response to National Security Risk Elevations
- All CCC devices must be password protected (or alternately protected by other appropriate Digital Team approved means such as Fingerprint and PIN).

BEHAVIOUR AND USE

- You must lock your device by using windows key and character 'L' whenever you leave your device unattended, regardless of your location
- You must not participate in unlawful, libellous, immoral, or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes the use of social media and 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.
- 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 Digital systems or equipment to the Digital 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.
- When working remotely, ensure Council devices are kept secure and not left unattended or visible in public places or vehicles.
- Access to Council systems from outside the UK requires prior approval from the Data Protection Officer and must be via a Council-approved device.

DEVICES

- You must not connect any non-authorized device to your CCC device, the corporate network, or corporate digital systems. This includes but is not limited to external hard drives, thumb drives, flash drives.
- The use of USB controlled peripherals such as screens, keyboards, mice, cameras and headphone / headsets are permitted.
- The use of a VPN (Virtual Private Network) is not permitted unless via prior agreement of the councils DPO and Head of Digital in exceptional circumstances. Use of a VPN without authorisation will result in the access being blocked.
- If you have a business case to support the need to print at home from a corporate device, this will need to be approved by the Councils Data Protection Officer and Head of Digital.
- Authorized devices are only those issued, managed and approved by Digital.
- You must not store any Council data on any non-authorized equipment.
- In order to comply with Data Protection legislation, all Council communications must only be made using Council approved applications and devices.

BRING YOUR OWN DEVICE (BYOD)

- Access to Council Systems via a personal device is limited to Microsoft 365 applications only (Outlook, Teams, Excel, Word, Excel, OneDrive, SharePoint and Microsoft Teams) and functionality is restricted.
- Access to your Corporate Microsoft 365 account and any third-party systems must be secured via Multifactor Authentication.
- Access to the Microsoft 365 applications is only permitted through the web versions. You can use the web versions to create, send and reply to Outlook emails and participate in Teams chats, meetings and calls.
- Printing any data from a personal device is prohibited this includes taking screenshots.
- Downloading of any Corporate data to any non-corporate device is prohibited, this includes copying and pasting from and to your personal device to corporate systems, this includes taking screenshots.
- Access to core line of business applications linked to your Microsoft login, should not be performed from personal devices. The downloading of documents or data from those systems to personal devices is prohibited, the only exception being the MySelf – iTrent HR platform.
- You are permitted to create, edit and save existing documents to OneDrive, SharePoint and Microsoft Teams.
- Personal devices should only be connected to the GUEST Wi-Fi and not those designated for Staff only use.

STORAGE

- You must not give or transfer data or software to any person or organisation, without a data sharing agreement and a completed Data Protection Impact Assessment (DPIA) approved by the Data Protection Officer.
- 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.
- The use of mobile devices such as memory sticks, CDs, DVDs, and removable hard drives is prohibited.
- The use of USB drives is prohibited for the storage of any corporate data. If there is a legitimate business need, a corporate encrypted USB device will be provided. Subject to approval by the DPO, Head of Digital and the SIRO.

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 Digital Team 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 to the Council and materials which are not copyrighted, or for which you have been granted use. The downloading and use of any non-approved software or application is not permitted
- You will need to undertake and pass mandated cyber security training before accessing Council Systems and Devices. This training is repeated and updated annually.
- New Starters (employees, and contractors) will need to undertake and pass mandated Cyber Security training before being provided access to Council Systems, this includes newly Elected Members.

WORKING REMOTELY

- Working away from the office must be accordance 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.
- Corporate devices must not be left in a vehicle overnight or for any prolonged period
- Laptops must be carried as hand luggage when travelling.
- Information and equipment must be protected against loss or compromise when working remotely.

WORKING ABROAD

- Access to Colchester Systems including Microsoft 365 accounts is blocked by default from non-UK locations.
- Working outside of the UK, first requires line manager, HR and Digital approval, Tickets must be logged in advance of travel with ICT.
- Members must log a ticket in advance but do not require HR or line manager approval and self-certify in this respect
- Working outside of the UK, approval is only granted to travel locations which are deemed as safe and compliant by both the DPO and ICT (based on ICO and NCSC guidance), the list of countries is annually reviewed and subject to change without notice based on geopolitical events and cyber risk.
- Only Corporate approved devices will be permitted when outside of the UK.
- Staff who use corporate accounts on BYOD devices should ensure that their corporate Microsoft 365 accounts are signed out of or deleted before travel to prevent unnecessary false alerts being raised.

USE OF SHAREPOINT / MICROSOFT TEAMS / MICROSOFT TEAMS

- You must not purposely engage in activity that may deprive an authorised user access to a SharePoint / Microsoft Teams resource.
- Use of SharePoint / Teams - Activity on SharePoint / Microsoft Teams may be monitored and audited to ensure compliance with Council policies.
- You must not circumvent SharePoint / Microsoft Teams 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 / Microsoft Teams in their area and are accountable for their actions.
- Site owners are responsible for the custody or operation of their SharePoint / Microsoft Teams sites and are responsible for proper authorisation of user access.
- Confidential or potentially sensitive data stored SharePoint / Microsoft Teams 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 / Microsoft Teams 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 / Microsoft Teams 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 / Microsoft Teams.

- 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.
- The sharing of documents externally should not be performed using open "Anyone" links and access must only be provided to listed trusted recipients.

USE OF MICROSOFT TEAMS

- Personal data should not be shared via teams messaging.
- Any data in Microsoft teams, sites, chats or meeting chat threads are subject to a Freedom of Information Request, Environmental Information Request and Subject Access Request.
- All users should ensure that permissions for documents are set appropriately.
- All users should ensure that retention periods for documents are set appropriately and in accordance with the retention policy and retention schedule.
- 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.
- The addition of external identities to Corporate Teams sites should only be performed after ICT approval.
- Only Corporate approved AI tools (i.e. Copilot) should be used and admitted into Corporate Teams meetings.
- Corporate Teams meetings should only be attended using Corporate Microsoft 365 identities and not personal ones, this also applies to Members.
- When attending third party created Teams Meetings caution should be taken when discussing personal, private or confidential council matters, which could be recorded and stored in a third-party Microsoft tenant, AI tooling can be used by the third-party and has become common practice.

MOBILE / SMART PHONES AND TABLETS

- 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 and text messaging is prohibited unless in exceptional circumstances.
- Any data contained on a work mobile may be subject to a Freedom of Information Request, Environmental Information Request and Subject Access Request.

- Employees are expected to use the internet responsibly and productively. Excessive personal internet browsing, including social media use, is not permitted.
- Corporate 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 are not permitted.
- Calls to overseas numbers need to be made via Microsoft Teams. This functionality can be activated for both laptop and corporate smart phones upon request but will need to be supported by an approved business case by a member of Senior Leadership Team and the Data Protection Officer.
- You must not use Colchester City Council mobile devices for conducting private business.
- Personal accounts and personal social media accounts should not be added to a Corporate mobile phone.
- 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 Regulation 110 of the Road Vehicles (Construction and Use) as amended March 2022, 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 Digital team Helpdesk immediately, you must also report and log this incident on the Data Protection Breach reporting system.

WHEN AN EMPLOYEE OR ELECTED MEMBER LEAVES

- It is the responsibility of the line manager / Democratic Services / alongside the and the Head of Service / Monitoring Officer to ensure the line manager to ensure the Digital Team are notified of any leavers or changes to staff roles (permanent, temporary or casuals) so that access can be terminated or amended as appropriate.

All Digital equipment, devices and data, remains the property of Colchester City Council and will be surrendered upon request or in accordance with our leavers process.

PASSWORD COMPLEXITY REQUIREMENTS

Passwords must meet complexity requirements settings. This setting determines whether passwords must meet a series of guidelines which are considered important for a strong password. Complexity requirements are enforced when passwords are changed or created.

Enabling this policy setting requires passwords to meet the following requirements:

- Passwords may not contain the user's Account Name value or entire Full Name. Both checks are not case sensitive.

Current guidance for the National Cyber Security Centre (NCSC) is to use three random words to create a strong memorable password. Numbers and symbols should still be used if

needed, for example Red-House-Monkeys-27. Be creative and use words memorable to you, so that people cannot guess your password. Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favourite sports team which are easy for people to guess. If you need help in generating a password, go to <https://correcthorsebatterystaple.net/>. It is recommended to use a minimum of 3 words and a minimum of 15 characters. If in doubt, reach out to the Digital Service Desk for guidance

Never use the following personal details for your password:

- Current partner's name
- Children's names
- Other family members' names
- Pet's names
- Place of birth
- Favourite holiday
- Something related to your favourite sporting team

With the use of Multi-Factor Authentication (MFA) and biometric fingerprint readers on laptops, the need to regularly change your password has been removed. This is based on NCSC guidance.

Digital reserve the right to force all users to change their password should the need arise.

Passwords must not be shared with anyone else and passwords should be completely different across systems and accounts.

PASSWORD SYSTEM SETTINGS

The following system settings relate to passwords:

- The users' previous 12 passwords are remembered
- Minimum password length is 8 characters (although we encourage a minimum of 15 characters, as above)
- Password must meet complexity requirements is set to Enabled

In the event of increased risk level as defined by GCHQ, NCSC and or Cabinet Office, tactical changes in line with recommendations from National Security Services may be implemented in real time.

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 constituting breach of this policy.

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

Compliance with this policy is monitored and all breaches of this policy will be investigated.

Where investigations reveal misconduct, disciplinary action may follow in line with the Council's disciplinary procedures.

Access to Council systems and devices may be suspended. Digital reserve the right to withdraw a users' access to any computer systems and communication services, including internet services without notice to protect the organisation as a result of identified Security and Data Protection Risks relating to use / breach of the acceptable use policy.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an employee, then the matter may be dealt with under the Councils disciplinary process. In relation to a Councillor in accordance with the Councillor Code of Conduct Arrangements.

POLICY REVIEW

In the event of increased risk level as defined by GCHQ, NCSC and or Cabinet Office, tactical changes in line with recommendations from National Security Services may be implemented in real time. This policy will be reviewed and updated as a result.

In any event the policy will be reviewed on an annual basis and updated as necessary at these reviews

VERSION CONTROL

Purpose:	To ensure safe and appropriate use of Council Digital Systems and Equipment.
Status:	Final
Final date:	16 th December 2025
To be reviewed:	November 2026