Acceptable Use Policy

October 2020

Customer Business Culture

Acceptable Use Policy

CONTEXT

We must act appropriately with the information we obtain and hold, and with the systems we use and access. How you use our systems, telephony, email and intranet 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 Borough Council must be aware of these policy statements and the obligations it places upon them.

Colchester Borough Council commits to informing all employees, members, voluntary workers, agency staff, contractors and other third parties of their obligations before they are authorised to access systems and information. Other organisations, and their users, granted access to technology managed by the organisation must abide by this policy.

This policy will be reviewed annually.

ACCESS TO IT SYSTEMS

- You must not allow anyone else to use your user username and password on 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 leave user accounts logged in at an unattended and unlocked computer.
- You must not attempt to access data 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 Policy.
- You must not access other people's email without their permission.
- You must not forward corporate emails to personal email accounts.
- 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 to ensure that only relevant parties are included.

PASSWORDS

- 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 complexity requirements:
    - Passwords must contain characters from three of the following categories:
        - Upper case letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
        - Lower case letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
        - A number from 0 to 9
        - Non-alphanumeric characters (special characters): (~!@#$%^&* -+=`|\(){}[]:;"'<>,.?/). Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.
        - Any Unicode character that is categorized as an alphabetic character but is not upper case or lower case. This includes Unicode characters from Asian languages.
    - Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value).
    - All CBC devices must be password protected.

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 organisation into disrepute. This includes publishing defamatory or knowingly false material about the organisation, colleagues or customers in any online publishing format.
- Only subscribe to services with your professional email address when representing the organisation.
- CBC 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 and co-operate with fault diagnosis and resolution.
- If you use our technology or our 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 the network or 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 Security Policy.
- Documents must not be stored locally (for example on c drive) on a desktop computer or laptop, as they are not backed up and information may be irretrievable if the device fails or is stolen. This includes synchronising SharePoint and OneDrive to a local device without ICT authorisation or on a secured CBC supplied device
- The use of mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be authorised by the Strategic ICT 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.

SECURITY AND LICENCING

- You must not attempt to disable or bypass anti-virus, malware or other security protection, and you should take care not to introduce viruses or malware. If you discover a virus or malware, you must notify ICT immediately.
- 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 Borough Council's 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.
- Information should be protected against loss or compromise when working remotely.

USE OF SHAREPOINT

- You must not purposely engage in activity that may deprive an authorized user access to a SharePoint resource.
- You must not attempt to access content for which you do not have permission.
- You must not circumvent SharePoint security measures. Corporate data/information must only be stored on team sites (not Office 365 groups).
- All staff must maintain the supported infrastructure setup by filing the documents via Adding Properties 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.
- Data used in 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.
- You must ensure that private or personal documents are secured (through the use of the 'only me' function) to ensure the security of information.
- Data can be shared with external people/organisations using the 'External sharing' SharePoint site. All documents shared must be removed once the need to share has expired. Any sensitive 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

- Only personal documents should be saved to OneDrive. OneDrive must not be used as a replacement for corporate shared document management, SharePoint.
- OneDrive documents, for example training notes, certificates, 121 meeting notes must not be kept for longer than necessary.

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.
- 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.
- 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 Assistant Director.
- You must not use Colchester Borough 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.

WHEN AN EMPLOYEE LEAVES

- Line managers must notify the ICT of any leavers or changes to staff roles 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 in the course of 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 security 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.

Also see

Information Security Policy

Data Protection Policy

Contact

ICT

ICT@colchester.gov.uk

01206 507340