Colchester City Council

Information Security Policy

August 2023

www.colchester.gov.uk

Information Security Policy

CONTEXT

Information is essential to delivering services to citizens and businesses. Information security refers to the defence of information or information systems from unauthorised or unintended access, destruction, disruption or tampering. It is important that the Council acts appropriately with the information we obtain, store and process. Confidentiality, integrity and availability of information must be proportional and appropriate to maintain services, comply with relevant legislation and provide trust to our customers and partners.

APPLICATION OF POLICY

Everyone who accesses information the Council holds must be aware of these policy statements and their responsibilities in relation to information security.

Colchester City Council commits to informing all employees, voluntary workers, agency staff, contractors, Councillors and other third parties of their obligations before they are authorised to access systems and information and subsequently at regular intervals. Other organisations, and their users, granted access to information held by Colchester City Council must abide by this policy.

This policy should be read in conjunction with the Acceptable Use policy and Data Protection policy.

All those who access information may be held personally responsible for any breach or misuse. For advice and support please contact ICT.

INFORMATION SECURITY PRINCIPLES

Information security is the preservation of:

- Confidentiality – ensuring that information is accessible only to those authorised to have access. To accomplish this, access to information must be controlled to prevent the unauthorised sharing of data, whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorisation are prevented from accessing assets important to the Council. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.
- Integrity – safeguarding the accuracy and completeness of information and processing methods. Integrity includes making sure data is trustworthy and free from tampering. The integrity of data is maintained only if the data is authentic, accurate, and reliable.
- Availability – ensuring that authorised users have access to information and associated assets when required. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to, and getting to the data should not take an inordinate amount of time.

ROLES AND RESPONSIBILITIES

The Organisation

- Ensures compliance with laws governing the processing and use of information

The Chief Executive

- Acts as Accountable Officer ensuring that all information is appropriately protected

Senior Information Risk Owner

- Promotes information security at senior management level

Technology Delivery Services Team

- Assures information security within the organisation
- Provides a central point of contact for information security
- Manages the investigation and mitigation of information security breaches
- Supports Information Asset Owners to assess risks and implement information security controls
- Ensures that staff are not able to gain unauthorised access to Council IT systems
- Ensures the security of the Council's IT systems, ensuring that access is restricted to staff with specific job functions
- Ensures that information security is assessed for all new systems and existing system developments including those provided by third party suppliers
- Ensures that a third-party specialist routinely reviews network security
- Ensures that no external agencies are given access to any of the Council's networks unless that body has been formally authorised to have access. All external agencies will be required to sign security and confidentiality agreements with the Council
- Ensure systems are protected, as far as reasonably possible, from external threat.

System Owners

- Ensures that appropriate information security controls are in place for each system under their control
- Ensure they delete or disable all identification codes and passwords relating to members of staff who leave the employment of the Council on their last working day
- Ensure that all new systems and changes to existing systems include the provision of appropriate information security controls (including those provided by third party) suppliers)
- Ensure that information security controls for each system under their control are documented

- Ensure that written backup instructions for each system under their management are produced. Backup copies should be held securely. Procedures should be in place to recover to a useable point after restart of any back-up
- Ensure that all systems are adequately documented and are kept up to date so that it matches the state of the system at all times.
- Ensure that a Privacy Impact Assessment (PIA) is completed for the use of any new systems or changes to existing systems
- Ensure that access to systems is limited only to those roles requiring access
- Ensure systems are protected as far as reasonably possible, from external threat
- No computer software (including cloud services) may be purchased by system owners without prior recorded authorisation from ICT.

Information Asset Owners

- Assess the risks to the information they are responsible for
- Help define the information security controls of the information they are responsible for, taking consideration of the sensitivity and value of the information
- Communicate the information security controls to authorised users and ensure controls are followed
- Ensure that a Privacy Impact Assessment (PIA) is completed when system changes involve data processing changes or before new personal data is collected or processed

All Managers must:

- Ensure their employees are fully conversant with this policy and all associated standards, procedures, guidelines and relevant legislation; and are aware of the consequences of non-compliance
- Develop procedures, processes and practices which comply with this policy for use in their service areas
- Determine which individuals are given authority to access specific systems. The level of access to specific systems should be on a job function need, irrespective of status
- Ensure that the relevant system administrators are advised immediately about staff changes affecting access (for example job function changes, leaving service or organisation) so that access may be withdrawn or changed as appropriate
- Ensure that staff are not able to gain unauthorised access to Council ICT systems or manual data
- Ensure all contractors and other third parties to which this policy may apply are aware of their requirement to comply
- Ensure that those users who have access to any part of the Council's Cash Receipting systems whereby they are taking payments either in person or over the phone should only enter card numbers into the relevant Capita payment screens and under no circumstances should Card Holder data such

as card numbers be written down or copied by anybody as this would breach The Payment Card Industry Data Security Standard (PCI DSS) compliance

- Ensure that where they cease using a third party hosted application that any data held by the supplier on behalf of the Council is either securely destroyed by the supplier or returned to the Council
- Ensure that if the Council vacates any of its premises, the manager of the service area occupying the premises must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all Council information is removed or securely destroyed.
- Ensure that service contracts adhere to Information Security policy standards.

Everyone must:

- Conduct their business in accordance with this policy
- Only access systems and information for which they are authorised
- Only use systems and information for the purposes authorised
- Comply with all applicable legislation and regulations
- Comply with information security controls communicated by the Information Asset Owner
- Not disclose confidential or sensitive information to anyone without the permission of the Information Asset Owner
- Ensure confidential, personal or special category information is protected from view or access by unauthorised individuals
- Not copy, transmit or store information to devices or locations (physical or digital) where unauthorised individuals may gain access to it; the security of devices and locations you use are the responsibility of the individual
- Protect information from unauthorised access, disclosure, modification, destruction or interference
- Ensure that unattended workstations are locked or logged out
- Keep passwords secret and do not allow anyone else to use their access to systems and accounts
- Notify the Technology Delivery Services Team of any actual or suspected breach of information security policy and assist with resolution
- Co-operate with compliance, monitoring, investigatory or audit activities in relation to information security
- Take responsibility for familiarising themselves with this policy and understanding the obligations it places on them
- Assist in protecting Council systems as far as reasonably possible from external threat e.g. phishing attempts and hacking attempts
- When disclosing personal or special category information to customers, particularly over the phone or in person, ensure that they verify their identity. Service areas dealing with customers on a daily basis should have suitable verification methods in place which must always be used
- Always secure laptops and handheld equipment and lock equipment away when leaving the office. Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Council property

- Physical security to all office areas is provided through the access control system. Staff should challenge strangers in the office areas without an ID badge. No one should allow anyone not wearing a valid ID badge to tailgate through security doors
- Staff working from home must ensure appropriate security is in place to protect Council equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Council equipment and information is kept out of sight. Council issued equipment must not be used by non-Council staff.
- Non CCC issued devices used to access Colchester Council systems will be treated as untrusted devices
- Access to systems from abroad is not permitted unless approved by the Data Protection Officer. Any access must be via a Council approved device.
- Users must not disclose any information related to ICT systems or security to any third party without the prior approval of ICT.
- Software and data purchased or licensed from external sources must only be used in accordance with the terms of the acquisition, licence, or other procurement documents.

ICT is responsible for maintaining the security and integrity of the Council's infrastructure and network by:

- Ensuring all parts of the network, at entry points and internally including wi-fi connections, are secured appropriately, following industry standards
- Ensuring that all user accounts are secured by the use of Multi Factor Authentication (MFA)
- Ensuring that all infrastructure components are secured to industry standards through managed permissions, firewalls and regular security, application and operating system patching
- Ensuring all infrastructure component, server and network devices, have up to date anti-virus application and tools installed
- Maintaining, patching, upgrading and updating via managed ITIL Change Control procedures
- Regularly conducting internal and external penetration tests and ensuring that outcomes are acted on appropriately and within required timeframes
- Ensuring that Global Administration and Administrator accounts are closely monitored and reviewed
- Enforcing security policies and taking appropriate action when any breach is detected or reported.

MONITORING

The organisation maintains the right to examine any system or device used in the course of our 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 manager and to the ICT team. If you are unsure, please contact ICT.

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

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 information security
Status:	Draft
Final date:	
Review date:	August 2024