Information security policy

Author: Gerardine Murphy, Head of ICT & Business Intelligence

Version 1.0
September 2020

Contents

1. Introduction & purpose

Information is essential to delivering services to residents and partners.

It is important that we at Colchester Borough Homes (CBH) act appropriately with the information we obtain and hold. Confidentiality, integrity and availability of information must be proportional and appropriate to maintain services, comply with the law and provide trust to our customers and partners.

Information security refers to the defence of information or information systems from unauthorised or unintended access, destruction, disruption or tampering. Information security is the preservation of:

- **Confidentiality** – ensuring that information is accessible only to those authorised to have access
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods
- **Availability** – ensuring that authorised users have access to information and associated assets when required.

At CBH we commit to informing all employees, Board members, voluntary workers, agency staff, contractors 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 us must abide by this policy.

This policy will be reviewed annually. All those who access information may be held personally responsible for any breach or misuse.

2. Roles and responsibilities

2.1 The Organisation

Ensures compliance with law governing the processing and use of information. The Chief Executive acts as Accountable Officer ensuring that all information is appropriately protected.

2.2 Senior Information Risk Owner (Director of Business Improvement)

- Assures information security within the organisation
- Promotes information security at executive management level
- Provides an annual statement about the security of information assets

2.3 CBH Strategic ICT Group

- Monitors the provision of information security by CBC Corporate ICT via a Service Level Agreement between CBC and CBH.
- Ensures that all system developments comply with Colchester Borough Council's ICT Strategy.

- Ensures all proposals for system developments and enhancements include consideration of security risks.

2.4 CBH ICT & Systems teams

- Provide a central point of contact for information security
- Support Information Asset Owners to assess risks and implement controls
- Manage the security of core business systems, ensuring that access is restricted to staff with specific job functions
- Ensure all identification codes and passwords relating to members of staff who leave the employment of CBH are deleted or disabled on their last working day
- Ensure that written backup instructions for each system under their management are produced. Backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a usable point after restart of this back-up
- Ensure that all systems are adequately documented and documentation is kept up to date at all times.

2.5 CBC Corporate ICT team

Via a Service Level Agreement between CBH and CBC, Colchester Borough Council ICT team is responsible for maintaining the security and integrity of the ICT infrastructure and network by:

- Ensuring all parts of the network, at entry points and internally including WiFi connections, are secured appropriately, following industry standards
- Ensuring that all infrastructure components are secured to industry standards though managed permissions, firewalls and regular security, application and operating system patching
- Ensuring all infrastructure component, server and network devices have up to date antivirus applications 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 on a weekly basis
- Enforcing security policies and taking appropriate action when any breach is detected or reported
- Managing the investigation and mitigation of information security breaches
- Ensuring that staff are unable to gain unauthorised access to ICT systems Ensuring that a third-party specialist routinely reviews network security
- Ensuring that no external agency is given access to any of the networks without formal authorisation. All external agencies will be required to sign security and confidentiality agreements.

2.6 Information Asset Owners

- Assess the risks to the information they are responsible for
- Define the protection measures of the information they are responsible for, taking consideration of the sensitivity and value of the information
- Communicate the protection controls to authorised users and ensure controls are followed.

2.7 Managers:

- 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 business areas
- Determine which individuals are given authority to access specific information 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 computer access (for example job function changes, leaving business unit or organisation) so that passwords may be withdrawn or changed as appropriate
- Ensure that staff are not able to gain unauthorised access to CBH 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 CBH or CBC's cash receipting systems whereby they are taking payments either in person or over the phone should only enter card numbers into the relevant 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 if CBH 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 CBH information is removed. Such checks should be documented, dated and signed.

2.8 Employees, Board members, voluntary workers, contractors and agency staff:

- 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 regulation
- Comply with 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 or sensitive information is protected from view 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 are the user's responsibility
- Protect information from unauthorised access, disclosure, modification, destruction or interference
- Keep passwords secret and do not allow anyone else to use their access to systems and accounts
- Notify the Head of ICT & Business Intelligence 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
- Take responsibility for familiarising themselves with this policy and understanding the obligations it places on them
- Reporting any breach, or suspected breach of information security without delay
- When disclosing personal or sensitive 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 security questions which must always be used
- Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when they are 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 CBH 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 and should not let anybody they do not recognise to follow them through security doors
- Staff working from home must ensure appropriate security is in place to protect CBH equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring CBH equipment and information is kept out of sight. CBH issued equipment must not be used by non-CBH staff.

3. Monitoring

We maintain 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.

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

4. References

CBC ICT & data protection policies

General Data Protection Regulations

Data Protection Act

5. Related documents

CBH ICT Acceptable Use policy

CBH Data Protection policy.

Document control sheet

Title	CBH Information security policy – September 2020					
File location	C:\Users\MurphyG\Colchester Borough Homes\Corporate Documents - Policy & Plans Development\CBH Information security policy.docx					
Consultation	Corporate management team CBC ICT ICT Support Manager Housing Systems Business Partner					
Approved	Board 01/09/2020					
Next review	01/09/2021					
Circulation method	Website, SharePoint					
Equality Impact Assessment	**Required**	No	**Latest**	[Latest EqIA (Full)]	**Review due**	[EqIA Review Due (Full)]

Document amendment history

Version	Type	Date	Notes
1.0	New	September 2020	New policy based on CBC Information Security policy