BHCC Policy Summary

1 Policy Name

Information Security.

2 Purpose of Policy

This policy is intended to protect the Council from security breaches to its information systems and the information stored on them.

3 Policy Summary

This is a framework policy which describes BHCC's approach to information security.

4 Critical Points

N/a.

5 Who does this policy apply to?

All authorised users.

6 Is acceptance of this policy mandatory?

Yes, this policy is mandatory for all users described in section 5 above.

Contents

7 Introduction

As public services look to more collaborative ways of working, recognising information as a valuable shared resource, the necessity for organisations to operate securely and adopt common standards increases.

Threats to information exist both internally through misuse, accidental or malicious loss or disclosure, and externally by hackers, disgruntled trouble makers or even foreign governments. Our customers expect that their information is held confidentially, is accurate and is available when and where it may be needed for their benefit.

Brighton & Hove City Council ('BHCC') is under various duties to adequately protect the information it holds about its citizens. There are various pieces of legislation that affect the Council such as the Data Protection Act, Freedom of Information Act, the Computer Misuse Act and the Human Rights Act. As well as legal duties the Council has contractual compliance obligations, such as the PSN Code of Connection. In order to comply the Council is committed to ensure these obligations are met and best practice and industry security standards are adopted and embedded throughout the organisation.

The primary tenet of policies, procedures and other mechanisms put in place by ICT is the protection of information and the systems containing information from illicit intrusion, damage, theft, corruption or unauthorised deletion. The Information Security Policy is an overarching policy that comprises information related policies, procedures, standards and other mechanisms, and draws them into one coherent framework. These policies detail the assertions, along with references to relevant guides and other supporting material, that have been enacted to ensure this duty is carried out efficiently and effectively.

Furthermore, these policies add value to the Council's activities by improving and optimising the Council's business processes and as a result increasing its efficiency.

BHCC will define and enforce this Policy Framework as a living document set enabling the Council to have an effective, consistent working environment with the ability to defend against internal and external threats and show due diligence to the people it serves. Effective information security ensures and increases public confidence and avoids any potentially damaging action being taken against the Council such as litigation or large fines from the ICO. The primary aim of the Information Security Policy Framework is to protect the Council from security breaches to its information systems and the information stored on them that might have an adverse effect on its operations, infrastructure financial position and/or reputation.

An Information Security Policy framework creates the working environment in which information is protected in an organisation. As a key dependency of an organisation's success information security must no longer be miscategorised as an ICT issue; it is not, it is a key business issue. A secure, consistent and reliable working environment operated by all members of staff, Members, partners and contractors is necessary to effectively contribute to enabling an organisation to reach its corporate objectives. The secondary objective is to position information as a key business asset and therefore a key business issue, thereby raising awareness and highlighting the importance of information security and ensuring that all employees, members and third parties are aware of their responsibilities.

8 Scope

This policy applies to all information in any format held on any media. This includes but is not limited to paper, electronic documents, email, fax, notes written on paper, audio and video recordings and conversation.

All Brighton & Hove City Council employees and Members shall familiarise themselves with this policy. All contractors and third parties should be made aware of, and agree to this policy during their period with the Council or during the period of access to the Council's systems

9 Policy

9.1 Principles

Information security includes protection of the following:

- Confidentiality: Ensuring that information and information systems are accessible only to authorised users.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorised users have access to information and information systems when required.

9.2 Risk

Non-compliance with this policy may result in financial loss, an inability to provide services to our customers, and adversely impact the Council's reputation.

9.3 General

BHCC shall use all reasonable, appropriate and cost-effective measures to protect its information and achieve its security objectives to ensure that information is appropriately protected.

BHCC has created the Information Security Policy Framework which can be visualised as a pyramid. This policy is the corporate overarching information security policy which states the organisations approach and commitment to information security; the top of the pyramid. This policy is underpinned by area specific policies such as Data Protection, information handling and remote working forming the second layer. These policies are based on the various standards with which the Council must comply. Policies are further supported by guidance, process and procedure at the third layer. The top 3 layers inform and are supported by the technology environment in which the organisation operates.

ISO 27001 / BS 7799 (Information Security Management and Records Management standards) will be used as the guide to determine policy and manage security.

The policy will comply with legal and contractual requirements including but not limited to:

- Computer Misuse Act (1990)
- Data Protection Act (1998)
- Environmental Information Regulations (2004)
- Freedom of Information Act (2000)
- IG Toolkit (N3)
- PSN Code of Connection (GCSx)
- Regulation of Investigatory Powers Act (2000)

The policy will not unnecessarily limit business or individual freedom, but take a balanced risk management approach.

Any security breach, or suspected security breach, must be reported to the ICT Service Desk immediately by telephoning 01273 29 2001 or by emailing ICT.servicedesk@Brighton-Hove.gov.uk. All reported incidents will be logged and investigated by the Information Security team in line with their current policy.

9.4 Monitoring

All users should be aware that in order to protect BHCC systems and to ensure that BHCC operates in accordance with its legal and regulatory obligations, system use may be logged and monitored in accordance with The Regulation of Investigatory Powers Act 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Communications sent or received by means of the Public Services Network ("PSN") may also be intercepted or monitored and users should understand the consequences of non-compliance with this policy and the Acceptable Use of ICT policy, which may include disciplinary and\or legal action.

9.5 Responsibilities

The Information Management Board ("IMB") is responsible and accountable for ensuring that the objectives of the security policy are met.

The Chief Technology Officer is responsible for implementation of the policy and is authorised to commission activities to achieve the policy objectives.

The ICT Security & Standards Manager has the responsibility to coordinate and control all the day-to-day activities associated with protecting the security of Brighton & Hove's City Council information.

The ICT Security & Standards Manager, in association with the Security & Standards Team and the ICT Department, is responsible for advising users on security issues, preventative monitoring of information systems and investigating security incidents.

The Data Protection Manager is the Council's designated Data Protection Officer. The Security & Standards Team will work with these officers to ensure compliance with these areas of legislation.

Key information systems have designated System Owners. These individuals are responsible for the security of their system and the data held on it. The Security & Standards Team will provide further advice.

All users of Council information systems are responsible for protecting information assets. Users must at all times act in a responsible, professional, ethical and security conscious way, maintaining an awareness of and conformance with the security policy.

10 Related Policies, Standards & Guidance

This policy should be read in conjunction with the following BHCC Policies:

- All other published BHCC ICT polices are relevant (see 14.1 for a full list)

This policy has been drafted in line with the recommendations and advice contained in the following documents:

- ISO 27002: Code of Practice for Information Security Management

The following is a non-exhaustive list of the statutes and statutory instruments deemed relevant to this policy:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

11 Terms & Definitions

12 Enforcement

Any user found deliberately contravening this policy or caught jeopardising the security of information that is the property of BHCC may be subject to disciplinary action and, where appropriate, legal action.

13 Review

This document will be reviewed annually as a minimum or wherever there may be a change of influencing circumstances.

14 Appendix I

14.1 Table of Information Security Policies

Policy	Current Version
Acceptable Use of ICT	5.04
Administrator Rights	1.04
Anti-Virus	1.03
Change Management	1.02
Data Protection	1.05
ICT Equipment - Disposal & Destruction	1.02
Email & Internet Usage	1.04
Encryption	1.03
Forensic Readiness	1.02
Incident Management	1.02
Information Handling	1.03
Information Security	1.05
Monitoring	1.01
Patching	2.03
Record Management	2.02
Remote Access	1.04
Removable Media	1.01

15 Document Attributes

15.1 Document Information

Policy Name	Information Security
Document Type	Operational Policy
Version	1.05
Date Created	11 November 2013
Last Review Date	24 September 2014
Next Review Date	30 September 2015
Document Author	ICT Security & Standards Manager
Document Owner	ICT Security & Standards Manager

15.2 Document History

Date	**Summary of Changes**	**Version**
11-11-13	New Policy	1.01
30-04-14	Change to Policy List & Typo's	to 1.05

15.3 Document Approval

Date	**Name & Job Title**	**Version**
30-09-14	Catherine Vaughan, Executive Director Finance & Resources	1.05

End of Document