BARNET
LONDON BOROUGH

Information Security Policy

London Borough of Barnet

Document Control

POLICY NAME	Information Security Policy		
Document Description	Policy which sets out the council's approach to information security, defines key roles and provides rules and guidance for staff and others to follow to ensure confidentiality, integrity and correct access to council assets and information.		
Document Author 1) Team and 2) Officer and contact details	1) Information Management Team 2) Sarah Laws, ext 2587 sarah.laws@barnet.gov.uk		
Status (Live/ Draft/ Withdrawn)	Live	**Version**	6.0
Last Review Date	New document – Dec 2014	**Next Review Due Date**	Jan 2016
Approval Chain:	Security Forum	**Date Approved**	19th December 2014

Version Control

Version number	Date	Author	Reason for New Version
1	Jan 2009	XXXXX	New Policy
2	Sep 2010	XXXXX	Formatting revision
3	27/07/11	XXXXX	Style updates and initial review by IMWG
4	31/08/11	XXXXX	Content update for IMWG Policy Map
5	19/09/11	XXXXX	Additional comments / contents
6.0 Draft	17/6/2014	XXXXX	Updates and amendments post new structure, law and practice changes
6.0	19/12/2014	Sarah Laws	Final version approved by Security Forum

Contents

1. Introduction

Information is a key asset for the London Borough of Barnet ("the council") and its correct handling is vital to the safe and effective delivery of public services. Information is held in physical and electronic ways. Physically held information includes paper copies, files and records etc. Electronically held information includes information in computers, drives, memory sticks, disks etc. These are all the council's information assets and are described more fully in 3.1.

The council needs to be confident that its information assets are safely and securely stored, processed, transmitted and destroyed, whether managed within the organisation or by delivery partners and suppliers. The council must also abide by the Data Protection Act 1998 (DPA) which governs how the council holds and uses personal data. The council's range of data protection policies are here. The council has a connection to the Public Sector Network which provides a secure network for organisations across central and local government and the wider public sector. Connection to this network is essential for the effective running of many council services. Our continuing access is dependent on us meeting a set of security and other standards.

The purpose of Information Security for LBB is to protect all its information assets. Implementation of this policy will provide assurance to stakeholders, partners and citizens that their information is held securely and used appropriately by the council, whilst complying with legislation and satisfying auditors.

2. Policy Definition

Any loss of computer systems or the information they contain could have serious repercussions for the council and / or its clients. A breach of security during processing, storage or transfer of data could result in financial loss, personal injury to a member of staff or client, serious inconvenience, embarrassment, or even legal proceedings against the council, and possibly the individuals involved.

The International Standard: ISO 27001 Code of Practice defines Information Security as the preservation of three aspects of information:

- Confidentiality: Making sure information is only available to correctly authorised people.
- Integrity: Making sure that the information cannot be corrupted or incorrectly deleted.
- Availability: Making sure that authorised users have access to information etc. when this is required

In order to ensure the confidentiality, integrity and availability of these systems an appropriate level of security must be achieved and maintained. The council will ensure that the level of security implemented on each of the various systems will be consistent with the designated security classification of the information and the environment in which it operates.

3. Scope and Responsibilities

Information security is not an option. We are all required to maintain a minimum level of information security to maintain our legal and contractual obligations.

3.1. Scope

The LBB Information Security Policy applies to:

- Everyone. The policy applies to all information held by the council which includes information held on its behalf by partners/contractors such as Re, CSG, NSL and all council Members, permanent, contract and temporary employees, and all third parties (for example employees of Re, CSG) who have access to LBB premises, systems or information. We refer to all these as “Everyone” in this policy.
- All council information. The policy applies to all systems, software and information created, held, processed or used on those systems or related media, electronic, magnetic, or written/ printed output from LBB systems. It also applies to all means of communicating information, both within the council and externally.

  Some examples of information that is covered by this policy:

  - data and voice transmissions or recordings,
  - post,
  - email,
  - sms/text,
  - cameras,
  - whiteboards,
  - memory sticks,
  - discs,
  - fax
  - image/sound processing,
  - video-conferencing,

- photocopying,
- flip charts,
- general conversation etc.

3.2. General Responsibilities

Everyone (see 3.1) must comply with this policy. These policies and standards must be included in service level agreements and contracts with ICT service providers.

Security breaches (or near-misses) caused knowingly, by reckless behaviour, or non-compliance with security policies including the non-reporting of an incident, will result in action being taken in relation to the conduct, capability or performance of the employee. This also includes accessing data without justifiable cause or for personal gain or interest.

Action may include formal action in line with the Council's policies and employee handbook. A severe breach, resulting in loss, maladministration or putting vulnerable clients at risk could constitute gross misconduct. It is the responsibility of each individual to understand where to find the latest policies and procedures for how the Council uses, processes and protects personal and sensitive data.

4. Specific responsibilities

The council as a whole has a number of responsibilities for information security. These are outlined below. Generally they are delivered by the IS Security Manager (IS) (or approved deputy) and the Information Management Team who work together on information security issues. Their roles also include developing policies to mitigate risk, and assisting with policy implementation into team procedures and standards.

4.1. Organisational Responsibilities for Information Security

The council has the following organisational responsibilities for information security:

- Ensuring that the relevant national and council guidance, security standards, procedures and guidelines are obtained, followed, disseminated, published and updated as necessary. The policies, guidelines etc. aim to reduce the risk of unauthorised modification, destruction or disclosure of information whether accidental or intentional. Within the council, access to information will be restricted to people who have a valid business need to know.
- Protecting information on computer systems by applying system patches and anti-virus software, which will be updated regularly. Scans will be carried out on all servers, workstations and laptops, and virus definitions will be automatically updated with manufacturer updates. Virus updates and scans will be automatic for every machine and must not be turned off or bypassed.

- Taking appropriate steps to prevent, detect, and recover from any loss or incident, whether accidental or malicious, including error, fraud, misuse, damage and disruption to, or loss of computing or communications facilities.
- Carrying out security risk assessments on information assets to identify the level of protection required. The security and control procedures required will take into account the sensitivity and value of the information.
- Investigating information security incidents reported to it – see the Security and Data Protection Incident Management Policy here for details.
- Providing a secure environment to store confidential waste pending collection by the shredding company. The council will ensure that any unsealed confidential waste bags will be sealed by the custodians.

4.2. Specific Organisational Roles

Within the council there are two organisational roles that have specific roles in relation to information security. These are the Senior Information Risk Owner (SIRO) and the Caldicott Guardian.

4.3. Senior Information Risk Owner (SIRO).

The SIRO is a senior officer who takes overall ownership of the council's information risk policy, acts as champion for information risk to the Strategic Commissioning Board (SCB) and provides written advice on the content of the council's Statement of Internal Control in regard to information risk. The SIRO is the Deputy Chief Operating Officer (DCOO).

The SIRO implements and leads the Information Management risk assessment and management processes and through the Risk and Assurance Manager advises SCB on the effectiveness of information risk management across the council.

The SIRO also plays an active role in determining whether any security policy exceptions meet the levels agreed in the policy exception process. For more detail on policy exceptions see the policy exceptions guidance note.

4.4. Caldicott Guardian

The Caldicott Guardian has a specific set of responsibilities for defining the circumstances in which personal information held about social care clients can be legitimately shared with other LBB business areas and delivery units and with other agencies. LBB has two Caldicott Guardians – one for Children's and one for Adults & Communities. The Children's Caldicott Guardian is the Head of Service Commissioning and Business Improvement and the Adults' is the Head of Social Care Commissioning. In LBB the Caldicott Guardians' responsibilities primarily relate to Social Care; similar roles exist in other agencies, such as the NHS trusts.

The Guardians are responsible for ensuring appropriate information sharing and advise on the different options to ensure lawful and ethical processing. In LBB the Caldicott Guardians work with the Information Management Team and the IS Security Manager.

4.5. Management

Managers have a number of responsibilities in relation to information security. These are as follows:

- In conjunction with HR, defining reference and vetting requirements for the role and undertaking pre-employment/contract reference checking. This includes managing clearance to HMG Baseline Personnel Security Standard for users who require access to the PSN.
- Ensuring that their staff fully understand this policy and all information management policies and guidance (available here).
- Developing compliant procedures, processes and practices for use in their business areas.
- Working with business continuity leads to maintain an appropriate Business Continuity Plan, which is incorporated into the corporate Business Continuity Plan, which can respond to all types of potential loss of critical infrastructure, systems and data and which covers the management of paper records and access to buildings during an incident, and ensuring their staff are aware of the plans for their area.
- Ensuring that when requesting or authorising access for their staff only the necessary authorisations are given and that required training is provided.
- Taking appropriate disciplinary action together with HR in the event of misconduct of non-compliance with this and related policies.

4.6. Responsibilities of Everyone

Everyone (see 3.1 above) who has access to LBB premises, systems or information must be aware of their responsibilities in ensuring the security and confidentiality of council held information. Compliance with all of the items detailed in 4. 7 is mandatory.

Everyone must familiarise themselves with this policy and comply with it.

- If you become aware of any actual or suspected breach of information security, or of any perceived weakness in this policy, or related procedures, practices, processes or infrastructure consult the Security and Data Protection Incident Management Policy for details of how to proceed. The policy is available here.

- If you are responsible for the management of third parties you must ensure that those third parties are contractually obliged to comply with this policy and are aware that their failure to comply may lead to contract termination &/or prosecution in serious cases.

4.7. Information Systems Security Requirements

- You must comply with all corporate policies, standards, procedures and guidelines with respect to information security.
- You must only access systems and information, including reports and paper documents, which you are authorised to access as part of your role.
- You must use systems and information only for the purposes for which they have been authorised.
- You must only access or attempt to access LBB systems from LBB ICT controlled or authorised secure equipment and approved software.
- All computer equipment, tablets blackberries, mobile phones, USBs etc. must be purchased through IS to ensure that they are appropriately secured before use.
- You must not connect or attempt to connect non Barnet approved equipment to LBB systems. However, authorised third party support contractors can use machines that are corporately owned and operated in accordance with acceptable ICT policies to support LBB systems. Contact the IS Security Manager for advice
- You must never leave computers logged into the network unattended unless password protected screen locking is available and has been enabled. This means that when you leave your desk you must lock the screen (usually by pressing the CTRL, ALT and DEL keys simultaneously, and then choosing the 'lock the computer' option from the menu)
- You must always 'shut down' your computer and ensure it is turned off before leaving the building.
- You must not store confidential electronic files and documents on your computer's local drive (C:) – if the computer crashes they may not be recoverable and the information will be lost as back-ups are not kept of information stored on local drives.
- You must not email council data, forward or divert emails to a personal email address, unless specifically permitted during a business continuity incident. This is because it is prohibited by the terms of the PSN connection, and also the safety of the information cannot be guaranteed.
- You must not use standard USB data sticks, CDs or other removable media as portable temporary storage for electronic files and documents unless they have been

encrypted. AES 256 standard encrypted USB data sticks may be used only after the Information Security Manager has approved a valid business case. These USB data sticks may only be purchased via the IT service desk.

- You must keep passwords and other access credentials secret, not write them down in any recognisable format and not allow anyone else to use your network account equipment or media in your care, or to gain access to any system or information.

- You must always beware of social engineering attacks (e.g. 'blagging') and establish the identity and authority of anyone requesting access to information or information system access, eg for servicing or repairs. You must only provide access or information if you are sure of the identity of the requestor, and that the access or provision of information is appropriate and lawful. If in doubt refer to the council's Data Protection Policy, Members Access to Information Policy, or ask your manager. You can contact IS (ext 3333), the Data Protection officer (ext 2029) or the Information Security Manager (ext 7117) for advice.

- You must not leave any valuables (computers, council IS equipment phones or similar council issued ICT equipment or peripherals) visible in the car. Get into the habit of putting them in the car boot even if you are not leaving the car unattended. Where possible do not leave valuables in the car overnight.

- If electronic media is no longer required, or if the user is leaving the council it must be returned to the service desk for appropriate disposal.

4.8. Security requirements for hard copy information

- You must never take business confidential material or documents containing personal information home, unless you are appropriately authorised to do so on a case by case basis Follow the Paper Records – Secure Handling and Transit Policy here.

- You must keep your desk clear of all paper files and documents when you are not working on them, to ensure their protection.

- You must maintain a clear desk policy when leaving your desk unattended for any period of time and out of office hours.

- You must keep all paper files and documents containing personal or business confidential information in secure, lockable cabinets. These cabinets must be kept locked, and the keys in secure locations. Cabinets must not be left unlocked for convenience. The location of keys must be kept confidential and not be easily accessible to non authorised persons.

- You must lock all laptops and paper files away in a secure cabinet when not in use in the office. Never leave them visible in the car. At home keep paper records in a safe place out of sight and separate from any valuables such as laptops

- If awaiting receipt of a fax which contains personal or business confidential information that is being received on a traditional fax machine you should stand by the machine while the fax is being received and immediately remove it, so that unauthorised individuals have no opportunity to see the information. You should always ring ahead to ensure there is someone at the other end to take receipt of the information, so information is not left unsecured at the other end.

- Only disclose business confidential or personal information with the permission of the information owner, or if required to do so by law or permitted to do so e.g. by an approved Information Sharing Agreement. See the council's Data Protection policies on the intranet for more information.

- In all cases it is the document holder's duty and responsibility to ensure the correct disposal of waste. See the Premises Security Policy for information on how this should be done.

4.9. Recommended good practice

Everyone is strongly recommended to follow the good practice detailed below.

- You should give up laptops and other council property if challenged for it during a robbery

- For personal items of value for example handbags, briefcases, rucksacks, other bags, wallets, purses, cash, other valuables, mobile phones etc:

- You should make a note of the serial and model numbers of personal items

- Do not leave these items where they are visible i.e. on desks or the floor near your desk/work area but put them away in the storage areas provided so that they are out of sight

- During office hours if you are away in meetings or lunch etc, put the items away and lock them up.

5. Reporting of Security Incidents:

Data Protection Incidents, Premises Incidents or Lost/Stolen/ Damaged Items

All IS, data protection and premises security incidents **must be reported immediately.** The details of how to do this and which incident should be reported to whom are contained in the Security and Data Protection Incident Management Procedure here .

6. Information Security Policy – Exceptions

Specific situations may arise where compliance with a particular aspect of this policy causes genuine business difficulties. If this is the case a request should be made for

a policy exception. Policy exceptions are exactly that – exceptions- and will not be approved routinely or as a matter of course. An overriding business need must be demonstrated for the exception to be granted. Refer to the *Policy Exceptions Guidance* for more information.

7. Review of Information Security Policy

This policy is a living document and thus updated periodically to reflect technological, legal and organisational changes. It should therefore be revisited on a regular basis by all staff.

The IS Security Manager in conjunction with the Information Management Team will review this policy on a yearly basis, or more often if technical, legal or procedural changes require more frequent revision. The policy will be available on the council's intranet on the Information Management Policies page here

8. Contact Information/Further Guidance

Further advice and guidance is available on general IS matters from the IS Service Desk and specialist security advice from the IS Security Manager

Tel No: service desk (020) 8359 3333
Email: IT service desk: ITServiceDesk@Barnet.gov.uk
Email: IS security: ICT.security@barnet.gov.uk

And on Data Protection and Information Management from the Information Management Team

Tel No (020) 8359 2029

Email: data.protection@barnet.gov.uk