INFORMATION SECURITY POLICY

1. INTRODUCTION

This Information Security Policy is intended to ensure that the Council complies fully with the requirements set out and applies to:

- All Council employees (temporary, part-time, agency staff)
- London Borough of Barnet Members
- Staff members of partner organisations (suppliers or contractors) who have been permitted access by the Council.

The purpose of the Policy is to protect the Council's **Information Assets** from all threats, whether internal or external, deliberate or accidental.

Information takes many forms and may be:

- Stored on computers, tapes, CD's or disks
- Transmitted across networks
- Printed out or written on paper & sent by fax
- Spoken in conversations and over the telephone.

Information Security Management enables information to be shared, while ensuring its protection. It has three basic components:

Confidentiality: Ensuring that information is accessible only to those who are authorised to have access.

Integrity: Safeguarding the accuracy and completeness of information and processing methods.

Availability: Ensuring that the Information is available as required to staff as need.

The scope of the policy is based on the Industry Standard ISO 27001, which is the international recommended code of practice for Information Security Management.

2. SECURITY RESPONSIBILITIES

The responsibilities for the Staff & Members (and partner organisations staff) are as follows:

- Council Directors Group is responsible for proposing and submitting to the Councillors, policies and standards relating to Information Security at LBB.

- The Information Governance Officer’s responsibilities include the overall co-ordination and management of the Information Security Policy and associated issues.
- Directors are responsible for ensuring that the Information Security Policy is applied within their services, and are responsible for delegating any administering responsibility.
- All staff & Members must adhere to this Information Security Policy.

All Council staff and Members must ensure that this guidance is implemented within the context of their role and employment by the Council.

Each system should have a nominated systems controller or "owner" who is responsible for determining who should have access to the systems either wholly or in part (restricted functions or data access).

Contracts with external suppliers of systems and services to the Council should have appropriate clauses to ensure that the suppliers conform to the Council’s needs and responsibilities with respect to Information security.

Any breaches of IT Security (e.g. theft, malicious damage to IT equipment or systems, compromise of security codes) must be reported as soon as possible as outlined in Section 13).

3. THIRD PARTY ACCESS TO THE COUNCIL’S FACILITIES

The objective is to maintain the security of the Council’s IT facilities and information assets, which are accessed by third parties (e.g. subcontractors, business partners and software suppliers).

The term “third party” generally refers to any non-LBB employed staff. Where there is a business need for such third party access, a risk assessment must be carried out to determine the security implications and control requirements. Controls must be agreed and defined in any contract with the third party.

4. STAFF ACCESS TO FACILITIES

Only authorised Council Officers may operate the Council’s IT equipment. Staff or external suppliers may only operate or access the Council’s systems with express permission from Information Systems (IS) and the appropriate Chief Officer. Staff must not bring onto Council premises any personal computer equipment and connect it to the Council’s network. On occasions external suppliers may come in and wish to link their laptops to our network. In these instances IS should be contacted who will authorise the connection.

All Service areas must maintain locally an Asset Inventory Log. This will contain details of all the equipment held in the area by the staff or kept in storage locally. The equipment could be any of the following:

- Computers

- Laptops
- PDAs or other hand held devices
- Mobile phones
- Printers, Scanners, Faxes, Projectors etc.

If you are in any doubt about this aspect please call the Service Desk.

All IT equipment used by the Council should have security facilities appropriate to the value of the equipment and the sensitivity of the data held. The security facilities provided must be used at all times appropriate to the facility. All the equipment should be security marked (Ultra violet and post code etching). All staff should activate the screen savers on their computers together with the password option, if this has not already been set by Information Systems.

IT equipment containing personal data must be sited and used in such a way that the data cannot be read by other staff or members of the public. Computer screens must not face windows or gangways where the information could be displayed and read without your permission. Where possible, computer systems must be ‘logged out’ at all times when you are away from your desk – i.e. meetings, lunch and especially at end of the working day. All computers must be switched off at the end of each day.

IT equipment may only be removed from the Council premises with permission. Records should be maintained by the service for their audit purposes

(Note for Managers: - When staff leave Barnet, the Service Link Officer should be contacted to check that all equipment that may have been taken by the staff member has been returned).

5. COMPUTER SYSTEMS AND SOFTWARE

IS systems must only be used for purposes directly concerned with the Council’s services, for which they are designated. This includes the Internet and e-mail facilities, which are provided for you. The Internet and e-mail Guidance outlines in more detail your responsibilities.

Only software authorised by Information Systems (IS) should be loaded onto the Council’s computers (do not load free CD’s, disks etc). All magnetic media (floppy disks and CD’s) must be checked for computer viruses before they are loaded onto computers.

Software must only be used in compliance with the terms of any contractual or license agreements.

All computer programs and data developed by or for the Council will remain in the sole ownership and copyright, and for the sole use of the Council except if explicitly decided otherwise by formal written agreement with Council.

Deliberate unauthorised access to, copying, alteration, or interference with computer programs or data is strictly forbidden under the Data Protection & Computer Misuse legislation.

6. NEW SYSTEMS AND SUPPORT

The objective is to ensure that security is built into information systems to minimise the risk of system failures.

The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements must be identified and agreed prior to the development of information systems. All security requirements, including the need for change control, audit trails, fallback arrangements and training needs, must be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case.

Acceptance criteria for new systems or services must be established and tested, prior to final acceptance and live implementation. Change control procedures must be in place for modifications to existing systems or services. This should ensure that the security procedures are not compromised, or where found lacking, are improved as necessary.

7. BUSINESS CONTINUITY

The objective is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. All Services must ensure that procedures are in place to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disaster, accident, equipment failures, and deliberate actions).
The process must:

- Identify risks (accidental and deliberate) and their potential impact
- Identify critical equipment, hardware and software and sources of data
- Develop, review and test business continuity plans (annually)
- Identify the insurance implications, e.g. covered for loss of data, software, and documentation, manuals etc.

Compliance

The objective is to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. The design, operation, uses, and management of information systems is subject to statutory, regulatory and contractual security requirements. Further guidance is available from Information Governance pages on the Intranet or the Information Governance Officer.

Regular reviews of the Council's Information Processing facilities and the associated procedures must be scheduled to ensure compliance with this guidance, and all necessary legal, statutory, regulatory and contractual requirements.

8. HANDLING & DISPOSAL OF INFORMATION

Personal information should not be disclosed or used other than as permitted by the appropriate Data Protection registration (see Data Protection Policy).

- Staff must refrain from casual browsing of personal data held in IT systems. Staff must not access computer systems to browse or update any data about themselves, their family, friends or other colleagues
- Staff must not browse, download, copy, store or distribute unsuitable (racist, sensitive, pornographic) material from the Internet. This is a serious breach of the Council policy, is likely to be a criminal offence, which will be reported to the police with possible disciplinary action
- Any personal data whether in printed form or on screens, should be kept secure and out of view when not in use. Where possible, screens should be positioned to ensure that other staff don't see the information on the screen.
- Staff should adopt a clear desk policy and put away all files and media every day (even during the day if you are going to be away from your desk for a long period)
- Secure copies of key data files should be taken and held in a secure environment at intervals appropriate to the type and criticality of the IT system and stored in a secure off-site facility. Regular housekeeping should be carried out on all data and any obsolete data should be deleted and/or archived (as per the Council's Records Retention Scheme). All documents and computer media must be clearly labelled and stored in a safe and secure location. Access must be restricted to authorised personnel
- Care must be taken when exchanging or sending information internally or externally and they should all have a confirmation of receipt. Media that are no longer required must be disposed of safely and securely. For further advice available from IS and the Intranet.
- The classification of information at the Council will comply with central government's procedures on security vetting and protective markings (Please see attached guidelines on this subject - **Security Vetting and Protective Markings** http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/DVA/DefenceVettingAgency.htm)

9. COMPUTER NETWORKS

The Council has numerous networks to which the computers and systems are connected. All network connections are set up by IS Staff. Staff must consult with IS staff if they have any requirements to change their network settings. Any failures or incidents must be must be logged with the Service Desk.

Network Access Control

The Council has procedures and technical controls in place to protect the facilities and the data passing through the network. Appropriate authentication mechanisms for users and equipment must be used, especially for remote access to the Council's network. All new services or equipment connected to the network must be approved by IS. This applies specifically to external suppliers and consultants who may need to connect to our network to demonstrate their products and services. All connections of this type must be cleared through IS – call the Service Desk to log your request.

10. ASSET INVENTORY

One of the major corporate responsibilities is to maintain an accurate inventory of all Council assets and associated nominated owner information.

Changes in the inventory, including configuration, location and users, must be reported promptly to the Service Desk.

11. EQUIPMENT DISPOSALS

Controls must be exercised over the disposal of redundant systems and software, including checks on ownership (some systems are leased), contractual limitations and deletion of data.

Information assets	Databases and data files, system documentation, user manuals, training materials, operational or support procedures, continuity plans, fallback arrangements, archived information.
Software assets	Application software, system software, development tools & utilities.
Physical assets	Computer equipment (e.g. processors, monitors, laptops, modems); communications equipment (e.g. routers, telephone systems, fax machines, answering machines); magnetic media (e.g. tapes/disks); other technical equipment (e.g. power supplies, air-conditioning units).

IS maintains an inventory of all computer-related hardware and software which is within the Council. All departments are responsible for ensuring that this is kept up to date and report any changes to IS.

IS will ensure that all Software and Data will be removed from computers which are to be disposed

Individual departments also have a responsibility to maintain a local inventory of their information assets

12. PHYSICAL SECURITY

Secure areas must be established for the most expensive and critical IT systems. Entry to the secure areas should be limited to authorised persons only, and due care must be taken to ensure physical security is maintained at all times. Access to sensitive or critical business information must be restricted and locked away when not required especially when the office is vacated.

Access codes, keys and other methods of entry must not be divulged or shared with unauthorised persons.

Appropriate measures for protection against fire, interrupted power supplies and other physical hazards must be in place for critical systems.

A clear desk and clear screen policy is recommended to reduce the risk of unauthorised access or damage to papers, media and equipment. Staff should not leave PDA's, laptops or mobile phones (or any personal equipment) unattended at any time. Staff must securely store these item(s) in the desks/cupboards provided to prevent theft. The Council accepts no responsibility in terms of replacing any personal items that are stolen or lost on Council premises. Staff will have to claim for personal items through their home and contents insurance. (See Appendix A for further guidance.) All Service areas must review the physical security arrangements and carry out risk assessments and implement appropriate solutions.

Responding to Security Incidents

Examples of security incidents are:

- Accidental or deliberate destruction, loss, modification or disclosure of information
- Unauthorised unavailability of systems
- Unauthorised access to information, including IT systems and telephone systems
- Misuse or unauthorised use of information
- Malicious damage to equipment
- Malicious software (including computer viruses)
- Theft of information or equipment (files, papers, floppy disks, etc).

Details of all information-related security incidents must be reported to the Information Governance Officer and the Service Desk.

The police must be contacted for cases relating to: theft and criminal damage, loss of identification cards or passes, and personnel incidents involving corruption, fraud, and unethical behaviour. A crime reference number must be obtained and passed to the CAFT team as soon as possible after the incident.

13. ACCESS CONTROLS & PASSWORDS

Staff Access Management

Formal procedures must be in place to control the allocation of access rights to systems and services. IS staff and Systems administrators must consider the following:

User registration	• Logs should be maintained of all staff access rights • Audit trails will record all transactions carried out by staff on the Council's systems (a Government Connect requirement)
Review of user access rights	• To maintain effective control over access to data and information services, IS and departmental IT managers must conduct a formal process at regular intervals to review users' access rights – every six months at least
User Password management and user responsibility	• The responsibility for issuing passwords for a service or a specific application must be clearly allocated both in IS and in client departments. • Where users are required to maintain their own passwords, temporary passwords must be issued initially, or when a user forgets a password. Where possible, a user should be forced to change a temporary password immediately.
Access Rights	• The responsibility for setting up, change and deletion of access rights rests with IS or system administrators where

	facilities allow.
Unattended user equipment	• All users must log out of services or applications when they have finished with them. Most computers can be secured using the CTRL+ALT+DEL facility. • All computer screens must be locked using the CTRL + ALT + DEL+ ENTER when users leave their desk.

All systems must have password controls, use trusted network logins or other appropriate security measures to ensure compliance with this policy. There may be some exceptions to this for accessing public or shared data for example the corporate telephone directory on the intranet. The rules on passwords are as follows:

- All passwords must be at least 8 characters (numeric, alphabetic, mixed case including special characters)
- Do not display/write down your password(s)
- Do not disclose your password to other staff/colleagues except in special circumstances
- Change passwords on a regular basis (every 4-6 weeks) and don't use common words (some systems will prompt you on a regular basis)
- Do give your password to your manager for use in emergencies (sickness, holidays etc) unless facilities exist to change your password to gain access without disclosing your password or access can otherwise be given. This should be provided in a sealed envelope, which the manager will need to store securely and use in emergencies only
- Passwords for staff that leave the Council or maybe transfer to work in another part of the Council should be deleted at the earliest opportunity. This is also a good opportunity to change the shared passwords for all the staff who are still in the section/department as the leaver may know the passwords
- The Password Security Policy provides further guidance in this area.

14. ANTI-VIRUS SOFTWARE

Virus detection and prevention measures must be in place to protect against malicious software such as computer viruses. It is Council policy that anti-virus software is pre-loaded on all computers. If you have any queries, please contact the Service Desk for further information.

The anti-virus software is automatically installed and updated, on all the Council's networked PCs.

Users of standalone PCs, home PCs or laptops where used for business, must liaise with IS to ensure that current versions of the approved Anti-Virus software is loaded on their machines and kept up to date.

15. STAFF RESPONSIBILITIES

Staff Recruitment

Security responsibilities must be addressed at the recruitment stage and suitable protections must be included in contracts of employment.

- Potential recruits must be adequately screened, especially for sensitive posts. Confidentiality agreements must be part of all employees' terms and conditions of employment. All third party users of information processing facilities must sign a confidentiality (non-disclosure) agreement.
- The Council's current procedures for recruitment are included in the Corporate Personnel Procedures.
- All contractors and external staff working on IT equipment and systems or in secure areas must be adequately vetted and monitored. They must also be made aware of the Council's Information Security, Internet, E-mail and Data Protection Policies.

Training and Awareness

The Council provides staff training in Information Security. Managers should ensure that all their key staff attend the training.

Personal Equipment

Staff must NOT bring their own IT equipment to work or use it for Council business, or use Council systems for private purposes.

Any breaches by staff of this policy will be dealt with under the Council's disciplinary code.

Aspects of Information Security are covered in the Council's Personnel Procedures Manual.

Homeworking

This applies to staff who work at home on a regular basis or those who take work home occasionally. This may include CD's, paper files, disks or information stored on Council laptops. All these assets (information and laptops) needs must be protected at all times as follows:

- All information (flash drives (memory sticks), disks, CD's & paper) must be protected and stored securely at all times whilst in transit and at home
- Do not leave your information lying around at home, put it away securely at all times – it could be damaged, lost or seen by other people who should not see it

- All laptops should have a boot password that must be enabled. Laptops in transit must be stored securely at all times (boot of car – not on the car seats)
- Switch off your laptop or desktop computer when you have finished your work – do not leave the computers switched on with information displayed on the screen. You could disclose personal/confidential information to your family or friends and this is a breach of the Data Protection Act and this guidance.
- If you require assistance or have any queries, please contact the Service Desk.

Staff Leaving the Council

Staff who leave the Council's employ must return, in working condition, all IT equipment, software, manuals, keys and other relevant items in their possession.

All the passwords for the staff member must be deleted at this stage.

16. SECURING INFORMATION

Back-up copies of essential information must be taken regularly to ensure that all essential business data and software can be recovered following a computer disaster, media failure or when otherwise required. This data must be stored in securely in a safe location.

Where possible, data files (word documents and spreadsheets) must be held on a central server so that the automatic backup schedules can be used. Back-up media must be regularly tested and stored securely, preferably in a different location to the main site. Staff are responsible securing (back-up's) of their information on their standalone computers and laptops.

Retention periods for essential business information, including archived copies, must be determined and followed at all times. The Council's Record Retention Scheme provides further details – contact the Information Governance Officer or Service Desk for further details.

Procedures and processes must be implemented for the timely restoration of critical systems in the event of disastrous loss of the hardware or data corruption.

17. DISCIPLINARY PROCESSES

This policy applies to all Council Staff and Members and must be followed at all times.

At the discretion of senior management, the Council's formal disciplinary process may be followed for employees who have violated this policy.
If you are unsure or require clarification about any aspects of this policy please contact your Manager or the Information Governance Officer.

IS Security Contacts

Information Governance x7080
0793-151-1931 (Mobile)

Resources – Service Desk - x7333

Corporate Anti-Fraud Team (CAFT) - x7988

Whistleblowing – Confidential Hotline - x2007

Relevant Policies

- Data Protection
- Internet & Email
- Acceptable Usage
- Password Guidance
- Data Transfer Security Policy

Appendix A

PERSONAL SECURITY GUIDANCE

All staff should follow the guidance outlined here to protect Assets (Information & Property) to prevent damage, theft or loss and personal injury

1. Property

The following table lists the types of items covered in this guidance.

PERSONAL PROPERTY	COUNCIL PROPERTY
Handbags / Briefcases	Laptops
Wallets / Purses / Cash / Other valuables	Personal Organisers (PDA's)
Mobile Phones / Personal Organisers	Mobile Phones
Memory Sticks (Flash Drives)	Memory Sticks (Flash Drives)

1.1 Good Practice

- *Staff should make a note of the serial and model numbers of their personal items*
- *Do not leave these items where they are visible i.e. on desks or the floor near your desk/work area*
- *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.*
- *The same rules apply for out of hours (evenings and week-ends)*
- *Staff should give up their laptops & other property if challenged in the street*
- *Do not leave any valuables (as above) visible in the car, get into the habit of putting them in the car boot even if you are not leaving it unattended*

1.2 Reporting of Lost/Stolen Items

In the unfortunate event of loss or theft of items one of the following processes should be followed. Obtain a crime reference number from the police, as this will be required for claim purposes.

- **Personal Property**

  Please report this to your manager, the police and your insurance company for claim purposes. The Council accepts no liability for any theft/damage to personal property.

- **Council Property**

  Please report this to your Manager, CAFT, Insurance, the Police and the Service Desk on 0208-359-7333 during office hours or 0208-202-4488 outside office hours.

2. Documents and files - Information

Staff should secure files, papers and data media (disks, CD's, memory sticks etc.) as these may contain confidential, sensitive and/or personal information. Staff should adopt a 'clear desk policy' out of office hours and during the day when they are not at their desk for long periods (during lunch and meetings etc.). All papers and media must be disposed of securely (shredding etc) to ensure compliance with this policy, Computer Misuse Act and the Data Protection Act. If in doubt please contact the Information Governance Officer or the Service Desk. Or check the Information Governance pages on the Intranet.