London Borough of Enfield

Members Information Security Policy

Author	**Mohi Nowaz**	Classification	**UNCLASSIFIED**	Date of First Issue	**28/05/2014**
Owner	**IGB**	Issue Status	**FINAL**	Date of Latest Re-Issue	
Version	**1.0**	Page	**1 of 15**	Date approved by IGB	
				Date of next review	**28/05/2015**

CONTENTS

1. Introduction

Information security means safeguarding information from unauthorised access or modification to ensure its:

- **Confidentiality** – ensuring that the information is accessible only to those authorised to have access;
- **Integrity** – safeguarding the accuracy and completeness of information by protecting against unauthorised modification;
- **Availability** – ensuring that authorised users have access to information and associated assets when required.

Information security is everyone's responsibility.

Enfield Council elected Members need to protect all information assets from the risks posed by inappropriate use. This includes protecting equipment and information from unauthorised or unlawful access, accidental or deliberate loss, damage, theft, disclosure or destruction.

This policy applies to elected members of the Council and will also apply to the following:

- Employees and agents of other organisations who directly or indirectly support or use the Council's Information Systems
- Temporary or agency staff directly or indirectly employed by the Council
- Users having access of any kind to the Council's systems, resources and/or networks

There is a specific Staff Information Security Policy which includes most of the content of this document.

This policy applies to all types of information, including, but not limited to:

- Paper
- Electronic Documents
- E-Mails
- Voicemail
- Text messages
- Web 2.0 records such as wikis, blogs and discussion threads
- Visual images such as photographs
- Scanned images
- Microform, including microfiches and microfilm
- Audio and video tapes, DVDs and cassettes
- Published web content (Intranet, Internet, Extranet, Social Media sites)
- Databases and information systems

Anyone who uses the Council's systems should be made aware of and be expected to comply with this policy and need to understand that the following UK and European legislation is relevant to information security:

Data Protection Act 1998

Freedom of Information act 2000

Computer Misuse Act 1990

Electronic Communications Act 2000

Copyright, Designs and Patents Act 1988

Human Rights Act 1998

Regulation of Investigatory Powers Act 2000

Telecommunications (Lawful Business Practice) Regulations 2000

A serious breach of this policy may lead to:

- withdrawal of ICT services
- A breach of the councillors' code of conduct and / or
- a criminal action being taken by the Police.

Compliance with this policy is part of your responsibility as a Councillor of Enfield Council. All incidents will be investigated and action may be taken in order to safeguard the Council and Councillors from legal action from residents, employees and statutory organisations.

2. Aims and Objectives

This policy aims to:

- Assist with raising the level of awareness of the need for information security as an integral part of the day to day business.
- Ensuring that Council Members are aware of and comply with the relevant legislation as described in policies and fully understand their own responsibilities.
- Ensure the Council's investment in information, software, hardware and other electronic resources is protected.
- Ensure the Council is compliant with law and government guidelines around information management.
- Safeguarding the accuracy, completeness and authorised accessibility of information and preventing unauthorised disclosure.

3. Using and Protecting our Assets

The Council encourages its stakeholders to seek innovative ways of using information technology in order to improve the way services are provided. This needs to be balanced with the need for information security, making sure that risk are managed and that assets are not used inappropriately.

The basic rules that apply are:

- The level of security required in a particular system, manual or electronic will depend upon the risks associated with the system, the data held on the system and the working environment of the system.

- A certain amount of limited and responsible personal use of our equipment is permitted. No Council assets or information can be used for your own commercial or business use or for political purposes (see Section 5).

- Enfield Council electronically audits computers, internet and email usage and random audits are also carried out when required.

- All information relating to our customers and business operations is confidential. You should treat paper-based and electronic information with equal care.

- Any correspondence, documents, records or handwritten notes that you create for Council related purposes, may have to be disclosed to the public under the Freedom of Information Act 2000 or the Data Protection Act 1998. Any comments recorded or notes written must therefore be professional.

Further information about using our ICT equipment can be found in the Acceptable Use Policy, available on the Member's Portal.

4. Provision of Council ICT equipment

The Council's ICT security arrangements are in line with central government's Public Services Network (PSN) Authority requirements, industry best practice (ISO 27001) and the Data Protection Act 1998. This document serves as an abridged version of the framework. As part of this, all councillors are required to sign the form in the **Privacy, Confidentiality, and Information Security Agreement** at the end of this document.

The Council provides councillors with technology to assist in the performance of their duties, which includes **laptops, iPads and Windows smart phones** together with software and materials provided for use with the computer. Anyone using the Council's equipment is required to undertake in writing that they observe and will comply with the procedures and protocols set by the Council as set out in this document.

Whichever choice is, or is not, selected, the Council will no longer automatically forward Council emails to personal email accounts such as hotmail, Google mail etc from 1 August 2014. This is to ensure the authority complies with the Government's PSN Code of Connection. Also, the Council will only send emails to a councillor at the @enfield.gov.uk email address.

The Council will provide a laptop or iPad that is technically secure, to enable the Councillor to access the internet, Corporate Email, Modern.Gov, Microsoft Office and necessary documents.

The Council provides the computer together with ancillary equipment and materials required, for the Councillor's functions as a Councillor. Use of this equipment by anyone other than a Councillor is not permitted.

Support for the device will be limited to resolving any issues with accessing Corporate information systems and will be provided by the authority's ICT section by telephoning the Customer Service Desk on 020 8379 4048 between the hours of 8.00 am to 5.00 pm – Monday to Friday. If you have any problems the equipment will need to be returned to the Civic Centre for inspection of faults, repair or replacement. Before coming into the Civic Centre please ring the VIP Support line on 020 8379 4048 to arrange an appointment.

All ICT equipment provided by the authority remains the property of the Council and must be returned at the end of the election term.

5. Using your Council ICT equipment

Councillors are required to act in accordance with the Council's requirements when using the resources of the Authority. IT equipment must not be used for purely political purposes but may be used where part of the purpose could reasonably be regarded as likely to facilitate or be conducive to the discharge of the functions of the Authority or an office to which the Councillor has been elected or appointed by the Council. Constituency work would be regarded as proper use of the facilities provided subject to notification to the office of the Information Commissioner under the Data Protection Act 1998 (see the 'Councillors and the Data Protection Act section below).

The Council is prohibited by law from publishing any material of a party political nature. If a Councillor uses their IT equipment for the preparation of material of a party political nature in pursuance of council duties they must do so in a way which is not attributable to, or appears to be on behalf of the Council. No costs should be incurred by the council as a consequence of publication of any party political material by a Councillor using IT equipment provided at the expense of the Council.

A Councillor must not use IT equipment provided in any manner which will prevent or interfere with its primary purpose as a facility to assist in the discharge of the functions of the Council. Accordingly, the Councillor must not:

a) misuse the computer in such a manner as to cause it to cease to function;
b) install or use any equipment or software which may cause the computer to malfunction.

The Councillor shall make reasonable arrangements for the safe-keeping of the computer.

a) laptops must be removed from a vehicle when it is left unattended
b) computer equipment must be placed away from windows
c) when not in use ICT equipment should be kept out of sight and preferably locked away

6. Using a Council issued laptop

If you are using a Council issued laptop then you will be able to access the Council's network from your laptop.

Information created or collected as part of working for Enfield Council is the property of the Council. For laptop users work related information should be saved to an individual's personal Documents folder on the Council network so that it can be stored securely.

Councillors must not store Council data on their own personal machines - data sets should only be accessed through the network.

The personal Documents folder is the property of Enfield Council. There should be no expectation of personal privacy on this Drive and the Council may require access to this folder with the approval of the Chief Executive.

Personal information about others held on the personal Documents folder is also subject to the Data Protection Act 1998 and may need to be disclosed to the person who the information is about, if they make a request to see it.

7. Using a Council issued iPad

If you are using an iPad then it is not possible to access the Council's network but you will still be able to access your Council email.

You will be able to store data on your iPad. You will also be able to save data on an externally hosted folder but please note that any documents that contain personal information or confidential Council information must not be stored externally.

8. Using Removable Media

The Council has a policy of restricting the use of USB sticks, digital memory cards and CDs/DVDs in order to meet our Privacy, Confidentiality and Information Security requirements.

A Council issued laptop will be able to read any USB stick, digital memory card or CD/DVD. You will also be able to copy files, images etc from these devices onto the network drive for work related purposes.

Using such media should be restricted to non-sensitive data wherever possible. However, in the event that you need to put sensitive data on removable media you should ensure that the data is encrypted.

The Council will provide you with a USB memory stick that will be encrypted and password protected prior to use. If you lose your USB stick you must report it as a security breach.

If you are using USB key/stick this can be achieved by the use of Council supplied encrypted USB sticks which prompt for a password whenever the key is inserted. The use of non-Council issued USB memory key/sticks is only permitted in the circumstances where you need to use a USB memory key/stick from a third party (e.g. someone from another organisation wishes to show a PowerPoint presentation). You may use this key only to read the required data from the device.

In the case of other devices such as CDS, DVDs the Data should be password protected using the software's (e.g. Word/Excel) own built-in mechanism or by creating a protected Zip file. Telephone the VIP Support line 0n 020 8379 4048 if you need further advice.

9. Reporting Security Incidents

An incident is an event that could cause damage to the Council's reputation, service delivery or even an individual. This could be a lost laptop or paper case file, a virus on the network or a damaged piece of hardware.

It is everyone's responsibility to ensure the safekeeping of any Council information or equipment in their control. Any theft or loss of any data or Council issued device used for Council business, email or containing Council related information must be reported to the VIP Support line or the ICT Security Analyst by completing the Information Security Incident / Risk Reporting Form, available on The Member's Portal. This needs to be done at the earliest opportunity.

The Council also needs to take action where potential incidents are identified. Where 'near misses' occur, these should be reported to VIP Support Manager and a local

decision taken as to whether the cause of the 'near miss' is one which could involve the enhancement of the policy or the process. If this is the case the Information Security Incident / Risk Reporting Form should be completed.

Please contact the VIP Support Manager for further information.

10. Internet Use

Enfield Council provides access to the information resources on the Internet to help Members carry out their role. The Internet must be used for lawful purposes only and you must comply with relevant legislation.

Internet access from the Council's network for personal use is at Enfield Council's discretion and should not be assumed as a given. Any misuse of this facility can result in it being withdrawn. Limited personal use of the Internet from a Council issued device is permitted.

We expect Members to use the Internet honestly and appropriately, to respect copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as in any other business dealings.

Further information about using Internet use can be found in the Email, Internet and Social Networking Usage Policy, available on Enfield Eye.

11. E-mail Use

The e-mail system is for Council business use only. However the Council understands that Members may also need to send or receive personal e-mails using their work address.

Council business by email can only be conducted using an Enfield email account (e.g. no Hotmail or Googlemail account can be used for Council business). Communicating with external individuals or organisations as required is permitted from the Enfield email account.

The Council will not allow the auto-forwarding of emails from a Council email account to an external email account used by a Member as this is in breach of the government's Public Services Network Code of Connection. Members will need to use their own personal email account if they do not wish to use the Council email account to conduct non-Council related Member duties.

Members will be provided with a Council issued laptop or iPad and a Windows smart phone to access their Council email and store a limited Council data in these devices. Data should be stored on the network as soon as possible to prevent loss of data if the device is lost or stolen. The devices will be encrypted to a standard required by the Public Services Network Code of Connection as well as the Information Commissioner's Office in order to meet the requirements of the Data Protection Act 1998.

Sending e-mails within the Council email system is secure. Sending e-mails externally is not secure and they can be intercepted and viewed by unauthorised people. Secure e-mail must be used when e-mailing information to external agencies or individuals when the content of the e-mail includes:

- Personally identifiable client or third party information

- Financial, sensitive or other information that could cause detriment to the Council or to an individual

Personal or sensitive business information must not be sent to an e-mail address outside of Enfield Council, unless it is absolutely necessary and the transmission is secure. This can be done using Egress Switch secure email and the Council can provide all Members with an Egress Switch account providing they use the Council email account.

Further information about transferring information securely can be found in the Email, Internet and Social Networking Usage Policy, and Secure Email Policy available on The Member's Portal.

12. Telecommunications

The Council may provide Telecommunication Services for Members to facilitate the performance of their work for Enfield Council. Users should not have an expectation of privacy in anything they create, send, or receive on telecoms equipment including Personal Digital Assistants (PDAs) and smart phones. However the authority of the Monitoring Officer or the Chief Executive will be sought before officers review any Councillors email and voice communications using Council equipment.

All use of phones must be in accordance with the Telecommunications Acceptable Usage Policy, available on The Member's Portal.

Details of calls made (e.g. sent to/from, date, duration and cost) are recorded on all mobile and most fixed line telephones. It will be assumed that all telephone calls or Short Message Service (SMS) messages made or received on Enfield Council equipment, are for business purposes unless the contrary is indicated.

It is everyone's responsibility to ensure the safekeeping of any telecommunications equipment in their control. Any theft or loss of any mobile device used for work email or containing work related information must be reported to the VIP Support Manager or the ICT Security Analyst by completing the Information Security Incident / Risk Reporting Form, available on The Member's Portal.

13. Access to Systems

It is a criminal offence under the Computer Misuse Act 1990, to deliberately attempt to access a system which you have no authority to access. ICT Services reserves the right to regularly monitor systems and unauthorised attempts at accessing systems may be investigated.

It is also a criminal offence under the Data Protection Act 1998 for any person to knowingly or recklessly obtain, disclose, sell or offer to sell personal information, without the permission of the data controller (Enfield Council). This is subject to certain exemptions. Full details about this offence can be found under Section 55 of the Data Protection Act 1998.

Members of the public and employees are entitled to see what information is held about them by Enfield Council. This includes handwritten notes, e-mails and any other information held electronically or in paper form. Always ensure that information is recorded in a professional manner.

Further information about Data Protection and its implication for information security can be found in the Data Protection Policy available on The Member's Portal.

14. Virus Control

Enfield Council seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software on laptops and PCs. It is a crime under the Computer Misuse Act 1990 to deliberately introduce malicious programmes into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc).

All Enfield Council computers have approved anti-virus software installed and this is scheduled to be updated at regular intervals. Users need to ensure that the anti-virus software is being updated on their devices and to report any problems with anti-virus updates.

Users of Enfield supplied computer equipment must be aware of the risk of viruses from email, internet and any removable devices inserted into their machine. Users should never download files from unknown or suspicious sources. All spam e-mails should be deleted and suspicious attachments or those from an unknown source must not be opened.

If you are in doubt about any data received or suspect a viruses has entered your PC, log out of the network immediately, stop using the PC and inform the ICT Service Desk on 020 8379 4888. You should always follow the instructions that the service desk issues about virus attacks.

15. Passwords

All users are given a unique Username and Password. Passwords should not be written down, kept where others might find them and must not be shared with anyone else.

The strength of your password will depends on the different types of characters that you use, the overall length of the password, and whether the password can be found in a dictionary. It should be 8 or more characters long.

All passwords must conform to the password standard which is as follows:

Password length must be a minimum of 8 characters and contain the following:

- At least one Numeric (0 1 2 3 4 5 6 7 8 9)
- At least one upper case (A B C D E F G H I J K L M N O P Q R S T U V W X Y Z)
- At least one lower case (a b c d e f g h I j k l m n o p q r s t u v w x y z)
- At least one special character (* ! # . @ # $ % ^ & * ,)

It is the Councillor's responsibility to ensure their password for accessing any Corporate Information service is not shared with any other person and that connection to such services is ended by logging off the system, as soon as work is completed or the connection is left unattended. This is to prevent unauthorised access to information.

If it suspected that someone else may know their password, or any security problem has occurred, Councillors must report this to the Customer Services Centre on 020 8379 4888 immediately so it can be rectified.

Further information on passwords can be found on the Access Control Policy, available on The Member's Portal.

16. Information Classification

Information classification or protective marking of information assets are used to:
• Determine the level of protection needed for the data
• Indicate that level of protection to other people
• Established a consistent approach to ensuring that data is appropriately protected.

To make sure that we neither over nor under protect information the Council has adopted the Government Protective Marking System. The Council uses the following three classifications:

UNCLASSIFIED or NOT PROTECTIVELY MARKED
PROTECT
RESTRICTED

The Council must not use the "Confidential", "Secret" or "Top Secret" classifications since this is reserved for Government use only and are subject to a very high level of information security. The Council will only receive "Restricted" information from the Government or agencies such as the Police.

Note - if a protective marking is not applied, the information will be considered UNCLASSIFIED.

The Council can use sub-categories to this classification if required, such as:

Descriptor	Description
PROTECT - COMMERCIAL	Material which relates to a commercial undertaking's processes or affairs.
PROTECT - MARKET SENSITIVE	Material which may reasonably be expected to affect a share price (e.g. material in Conclusions and Summary of a draft inquiry report).
PROTECT - PERSONAL	Material which should only be seen by the individual to whom it is addressed (e.g. a letter on a pay award, or disciplinary action).
PROTECT - STAFF	Material exchanged between managers, where references are made to named or identifiable individual(s) (e.g. a discussion on plans to reallocate staffing roles). LBE includes in this descriptor Members and third-party contractors, their directors, partners and employees.
PROTECT - MANAGEMENT	Material which concerns policy and planning affecting the interests of groups of employees, members or third-party contractors.

PROTECT - APPOINTMENTS	Material concerning actual or potential appointments that have not yet been announced.
PROTECT - CONTRACTS	Material concerning tenders under consideration and the terms of tenders accepted.

These descriptors can also be used with RESTRICTED.

Paper documentation with business critical information on should not be taken off site, particularly if it has protective marking applied. Where paper documentation is taken off site this must be securely locked away when not in use.

All data marked as “PROTECT” or above stored on any removable media must be encrypted.

Further information about information classification can be found in the Information Classification Policy available on The Member’s Portal.

17. Security of Equipment

Users are required to screen-lock their computers when leaving the room, for any length of time. To lock your computer screen, press the Windows key + L key at the same time.

Unsecured laptops and other portable equipment should never be left unattended. You should lock your laptop using a laptop security cable lock when left unattended but it is good practice to lock it at all times to help prevent it from being stolen. It is your responsibility to ensure that adequate safeguards are taken to protect your equipment.

All confidential or sensitive information held in paper form, should be shredded or ripped up and placed in the ‘confidential waste sacks’ located in Council buildings, when they are no longer required. Personal or sensitive information must not be disposed of in the black general waste sacks. These sacks are not held or disposed of securely and can be accessible to the public.

All confidential documents that have been sent to a shared printer should be collected immediately, to ensure they are not picked up or read accidentally or deliberately by someone not authorised to see the information.

Further information about using security of equipment and information can be found in the Acceptable Use Policy, available on The Member’s Portal.

18. Remote Working

Working remotely can pose several security risks. To help reduce these risks, you should ensure you carry out the following:

- Position yourself so that your work cannot be overlooked by others not authorised to see the information.

- Take precautions to safeguard the security of any computer equipment on which you do Enfield Council business, and keep your passwords secret.

- Inform the Police, the VIP Support Manager and the ICT Security Analyst as soon as possible if any sensitive paperwork or computer equipment has been stolen or lost and complete the Information Security Incident / Risk Reporting Form, available from The Member's Portal.

- Ensure that any work you do remotely is saved on Enfield Council's network or is transferred to it as soon as possible.

- Ensure that secure ID tags or memory sticks are kept separately from computer equipment when not in use.

- Computer equipment should not be left on view in vehicles, public transport or hotels or left in vehicles overnight.

Remember that these rules apply equally when you working at home. Not even a member of your family should have access to Enfield Council's information.

19. Disclosure of Information

Personal or sensitive business information held by Enfield Council must not be disclosed to anyone internally or externally, unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information. Verification can be sought from the Council's Information Governance Board when this is not clear. To learn more about sharing information, refer to the Information Handling and Protection Policy, available on the Member's Portal.

If you have received a request for information from a member of the public, or another organisation and they mention the Freedom of Information Act 2000 or the Data Protection Act 1998, contact your VIP Support Manager for further advice if it involves Council information.

Further information about this can be found in the Freedom of Information Policy and the Data Protection Policy available on The Member's Portal.

20. Physical Security

Council office areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access. All members are required to wear visible identification.

Further information about this can be found in the Physical and Environmental Security Policy, available on The Member's Portal.

21. Disposal of Computer Equipment

If you have any redundant, faulty or unused hardware or software, contact the Enfield IT Service Desk on 020 8379 4048. Do not dispose of this yourself. The disposal of all IT equipment e.g. PC's, printers, laptops, tablet PCs, PDAs etc must be carried out in a secure manner to ensure that no data is left on devices that can be retrieved after disposal.

LONDON BOROUGH OF ENFIELD
Privacy, Confidentiality, and Information Security Agreement

As a user of Enfield Council's IT systems and data, I understand that I am responsible for the security of my User ID (login) (s) and Password(s) to any computer system for which I am granted access. I understand that I have the following responsibilities:

- Adhere to the Council's information security policies & processes
- Follow security procedures for the information systems I access
- Use only software authorised for use and prevent the introduction of unauthorised software
- Choose effective passwords and log on to Council systems using my own ID and passwords only
- Not give my password to anyone else to log into the network or business systems and ensure that the password is not written and accessible to anyone else.
- Ensure that I lock my computer screen when it is left unattended
- Accept accountability for all activities associated with the use of my individual user accounts and related access privileges
- Ensure the security of any computer equipment taking appropriate measures such as cable locks and storage in lockable cupboards to secure equipment at work location and off site
- Not to change the computer configuration unless specifically approved to do so
- Take appropriate precautions against viruses
- Use email, public networks and the Internet in a professional manner
- Maintain the confidentiality of information disclosed to me as part of my duties, even when I am no longer an elected Member
- Report policy violations, security breaches or weaknesses to the appropriate person
- Not download any personal information about staff or customers to any unencrypted removable media
- Maintain an awareness of UK information legislation and ensure that all information is processed in accordance with the Data Protection Act 1998.
- If I am about to leave the council, I will inform Democratic Services prior to departure of any important information held in my account and manage my account in accordance with the council's email and records management policy.
- I acknowledge that my use of the network may be monitored for lawful purposes.

I understand that where I have access to or use of information classified as PROTECT or RESTRICTED, additional protections are expected.

I understand that I must maintain and safeguard the confidentiality of any and all PROTECT and/or RESTRICTED information accessed or obtained in the performance of my authorized duties or activities. I will not access, use, and/or disclose PROTECT and/or RESTRICTED information for any purpose other than the performance of authorized activities or duties. I will limit my access, use and disclosure to the minimum amount of information necessary to perform my authorized activity or duty.

I have been given access to all of Enfield Council's Information Security Policies and Guides relevant to my role as an elected Member.

In order to fully understand my responsibilities with respect to Privacy, Confidentiality and Information Security I undertake to complete the following training course:

Data Protection Act

I understand that failure to comply with the above Privacy, Confidentiality, and Information Security agreement may result in denial of access to information and termination of my access to the London Borough of Enfield's ICT services.

Policy Declaration

I confirm that I have read, understood and will adhere to Enfield Council's Members Information Security Policy.

By signing this Agreement, I understand and agree to abide by the conditions imposed above.

Signature: ……..

Name: …….

Council Ward: ……

Date: ……...

To be retained by Democratic Services