London Borough of Enfield

Members Information Security Policy

Author	**Mohi Nowaz**	Classification	**OFFICIAL - PUBLIC**	Date of First Issue	**28/05/2014**
Owner	**IGB**	Issue Status	**DRAFT**	Date of Latest Re-Issue	**23/11/2015**
Version	**1.8**	Page	**1 of 19**	Date approved by SWG	
				Date of next review	

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's 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.

There is also 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

All members using 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 Code of Conduct for Members 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.

Breaches of this policy may amount to a breach of the Council's Code of Conduct for Members. The application of this policy shall be a matter for the Council and for the Councillor Conduct Committee and, as appropriate, the Monitoring Officer, acting in accordance with their terms of reference.

A formal complaint may be made to the Monitoring Officer, who will review the complaint, consult with appropriate parties and then give their decision on how the complaint will be dealt with.

Additionally, violations of this policy, such as breaching the Data Protection Act, could lead to fines being issued and possible criminal or civil action being taken against the Council or the individual(s) involved.

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 risks 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 record 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.

The Council will provide a laptop or iPad that is security hardened, 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 to whom it is issued 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.

Only Council equipment will be supported by the Customer Service Desk. The Council cannot provide any support for a Member's own personal equipment.

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 of an office to which the councillor has been elected or appointed by the Council. Constituency work, for example, is regarded as proper use of the facilities provided, subject to notification to the Office of the Information Commissioner under the Data Protection Act 1998.

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, or the Council provided externally hosted OneDrive folder if available.

Councillors must not store Council data on their own personal machines - data sets should only be accessed through the network. Please note that any documents that contain personal or confidential Council information must not be stored externally on member's own device or a personal hosted storage service such as OneDrive, Dropbox, Amazon etc. as these services may store data outside of the European Economic Area.

All data stored on Council equipment, including laptops, iPads and the personal Documents folder or the Council provided OneDrive 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 all drives and folders to carry out its investigations 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 the Council provided externally hosted OneDrive folder. Please note that any documents that contain personal or confidential Council information must not be stored externally on member's own device or a personal hosted storage service such as OneDrive, Dropbox, Amazon etc. as these services may store data outside of the European Economic Area.

All data stored on Council equipment, including laptops, iPads and the personal Documents folder or the Council provided OneDrive 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 all drives and folders to carry out its investigations with the approval of the Chief Executive.

Personal information about others held on the personal Documents folder or the Council provided OneDrive 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.

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 must 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 on 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 on 020 8379 4048 immediately so that action can be taken to limit any potential loss of data and costs.

Once the incident has been reported to the VIP Support line as above, the Information Security Incident / Risk Reporting Form, available on The Member's Portal, needs to be completed and sent to the Information Security Analyst as detailed in the form. 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 line on 020 8379 4048 if you need further advice.

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. Reasonable 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.

All existing Council policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of Council resources, sexual or racial harassment, information and data security, confidentiality, and those included in the Code of Conduct for Members.

Council systems and equipment, including email and Internet systems and their associated hardware and software, are for official and authorised purposes only. However, personal use is authorised where it:

- does not interfere with the performance of your official duties

- is of reasonable duration and frequency
- serves a legitimate Council interest, such as enhancing your special interests or education
- does not overburden the system or create any additional expense to the Council.

You should consider carefully discretionary use for any other purpose.

You may use the Council's Internet facilities for personal purposes as set out above, but you may not access any obscene or pornographic sites, and may not access or use information that would be considered harassing. Council facilities must not be used in an unlawful way.

A wide variety of materials may be considered offensive by colleagues, customers or suppliers. It is a violation of Council policy to store, view, print or redistribute any document or graphic file that is not directly related to your role as Councillor or to the Council's business activities. This should be understood with reference to the Council's policy framework, including the Equal Opportunities policy.
Some uses of the Council connection to the Internet can never be permitted. Internet use is inappropriate when it:

- Compromises the privacy of users and their personal data
- Damages the integrity of a computer system, or the data or programs stored on a computer system
- Disrupts the intended use of system or network resources
- Uses or copies proprietary software when not authorised to do so
- Results in the uploading, downloading, modification, or removal of files on the network for which such action is not authorised

It is impossible to define all possible unauthorised use. However, examples of other unacceptable Internet use include:

- Unauthorised attempts to break into any computer or network
- Using Council time and resources for personal gain
- Theft or copying of electronic files without permission
- Sending or posting Council confidential information outside the Council or inside the Council to unauthorised personnel
- Refusing to cooperate with a reasonable security investigation
- Sending chain letters through email

All Council Internet users are prohibited from transmitting or downloading material that is obscene, pornographic, threatening, racially or sexually harassing, or in any way contravenes the Equal Opportunities policy.

Further information about using internet use can be found in the Internet and Email Usage Policy for Councillors, available on the Member's Portal.

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 Google mail account can be used for Council business).

Communicating with external individuals or organisations as required is permitted from the Enfield email account.

The Council does not automatically forwards Council emails to personal email accounts such as Hotmail, Google mail etc. This is to ensure the authority complies with the Government's Public Services Network (PSN) Code of Connection. Also, the Council will only send emails to a councillor at the @enfield.gov.uk email address.

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 amount of Council data on 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 PSN 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 secure email guidance available using Egress on The Member's Portal.

12. Social Media

Social media is the term used for online tools, websites and interactive media that enable users to interact with each other by sharing information, opinions, knowledge and interests. Applications include for example, but are not limited to:

- Blogs, for example, Blogger
- Online discussion forums, such as Ning
- Media sharing services, for example, YouTube
- Applications such as Facebook, Twitter, Google+ and LinkedIn

Members must ensure that they use social media sensibly and responsibly, in line with corporate policy. They must ensure that their use will not adversely affect the Council or its business, nor be damaging to the Council's reputation and credibility or otherwise violate any Council policies. The following risks have been identified with social media use (this is not an exhaustive list):

- Virus or other malware (malicious software) infection from infected sites.
- Disclosure of confidential information.

- Damage to the Council's reputation.
- Social engineering attacks (also known as 'phishing').
- Bullying or witch-hunting.
- Civil or criminal action relating to breaches of legislation.
- Breach of safeguarding through the use of images or personal details leading to the exploitation of vulnerable individuals.
- Breach of the code of conduct for members through inappropriate use.

In light of these risks, the use of social media sites should be regulated to ensure that such use does not damage the Council, its employees, councillors, partners and the people it serves.

Members are personally responsible for the content they publish on any form of social media. Publishing or allowing to be published (in the form of a comment) an untrue statement about a person which is damaging to their reputation may incur a libel action.

Social media sites are in the public domain and it is important to ensure you are confident of the nature of the information you publish. Once published, content is almost impossible to control and may be manipulated without your consent, used in different contexts, or further distributed.

Members should make use of stringent privacy settings if they don't want their social media to be accessed by the press or public. Read the terms of service of any social media site accessed and make sure you understand their confidentiality/privacy settings.

Do not disclose personal details such as home addresses and telephone numbers. Ensure that you handle any personal or sensitive information in line with the Council's Data Protection Policy.

Do not publish or report on meetings which are private or internal (where no members of the public are present or it is of a confidential nature) or are Part 2 reports (which contain confidential information or matters which are exempt under the provision of the Local Government (Access to Information) Act 1985).

Copyright laws still apply online. Placing images or text from a copyrighted source (e.g. extracts from publications or photos) without permission is likely to breach copyright. Avoid publishing anything you are unsure about or seek permission from the copyright holder in advance.

Don't send or post inappropriate, abusive, bullying, racist or defamatory messages to members of the public, other councillors or officers either in or outside the work environment.

The Council will not promote councillors' social media accounts during the pre-election period.

In any biography, the account should state the views are those of the councillor in question and may not represent the views of the Council.

Do not use the Council's logo, or any other Council related material on a personal account or website.

Social media must not be used for actions that would put councillors in breach of the Council's Code of conduct for members. For example, don't publish on social media something you wouldn't say face to face, or at a public meeting.

Be aware of your own safety when placing information on the internet and do not publish information which could leave you vulnerable.

Anyone receiving threats, abuse or harassment via their use of social media should report it to their political group leader, members' services and/or the police.
It is recommended that in the case of Facebook, councillors wishing to keep their personal life and role as a councillor separate create a Facebook page which members of the public can like rather than using their personal profiles.

Councillors are reminded that in respect of social media, they are governed by the Code of conduct for members and relevant law.

The Council reserves the right to request the removal of any content that is deemed to be in breach of the Code of Conduct for Members.

13. 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 councillor's 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.

Internet Usage and access from Mobile Smartphones and Tablets and connecting by Enfield Council Mobile data contracts is included in this policy. Use of mobile Apps is also intended for business purposes and included in this policy.

Only software purchased by Enfield Council and approved by Corporate IT may reside on Enfield Council computer equipment including PDA's and smart phones.

Calls, texts and data usage on mobile phones should only be for business purposes. Data limits are set on Mobile Sim Contracts, and excessive usage over these limits and out of normal working hours or usage abroad will be subject to interrogation. You may be liable to pay charges incurred if usage cannot be shown to be for Council business.

If Council equipment is being used abroad (see Section 15. Access from Overseas) then Members should use Wi-Fi services wherever possible if this is deemed to be safe in order to avoid excessive charges being incurred, particularly outside of the European Economic Area (EEA). If Wi-Fi services are not viewed as secure then Council equipment must not be used to access the Council network and email system. Connecting to an unknown publicly available Wi-Fi and sending emails or

logging into systems can expose usernames, passwords and confidential information to criminals.

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.

14. 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.

15. Access from Overseas

Access to the Council's network from overseas is subject to additional controls to ensure compliance with relevant legislation, including the Data Protection Act, and this may place additional personal liability on to Members.

Members visiting countries within the European Economic Area (EEA) can use their Council equipment to carry out Council business and access the Council's network. In order to avoid roaming charges, Members should only use secure Wi-Fi networks that require authentication when accessing Council data. If Wi-Fi services are not viewed as secure then Council equipment must not be used to access the Council network and email system. Connecting to an unknown publicly available Wi-Fi and sending emails or logging into systems can expose usernames, passwords and confidential information to criminals.

If roaming services are required then a written request including a business case must be submitted to the Monitoring Officer for consideration at least a month in advance of any planned overseas travel. Any charges arising from the use of Council equipment from abroad may have to be paid by the user if prior approval for use has not been granted.

Members are their own Data Controllers and as such have responsibility for any personal data involving their residents that they may access from abroad and need to ensure that any access to resident's personal data do not breach the requirements of the Data Protection Act, particularly if they are visiting outside of the EEA.

The facility to remotely access the Enfield network from outside of the European Economic Area will only be permitted in exceptional circumstances and should not be assumed. A written request including a business case must be submitted to the Monitoring Officer for consideration at least a month in advance of any planned overseas travel, including a request for roaming services if this is required. Any charges arising from the use of Council equipment from abroad may have to be paid by the user if prior approval for use has not been granted. In some non-EU countries these costs may be significant.

Members should seek advice from the IT Security Analyst before taking any Council supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the Council's normal insurance against loss or theft.

It should be noted that in some overseas territories electronic devices can be confiscated by customs on arrival and should not be used close to security service facilities – including police stations, check points and the like. It might be worth checking this prior to departure.

16. 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 4048. You should always follow the instructions that the service desk issues about virus attacks.

17. 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 Council IT 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 VIP Support line on 020 8379 4048 or 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.

18. Information Classification

Information is a valuable asset and aids a local authority to carry out its legal and statutory functions. The information that the Council processes can be highly confidential and very personal and therefore the Council has a legal duty to take care of it. Like any other strategic asset, information must be protected appropriately depending on the level of sensitivity of the information.

The new Government Security Classification Policy (GCSP) came into effect as from 2nd April 2014 and replaces the old Government Protective Marking Scheme (GPMS) that was in place prior to that date.

The Council has adopted the Government's revised information classification policy which moves from the three levels of classification that the Council was using to the OFFICIAL classification for all Council information.

All Council information will be classified as OFFICIAL. This recognises that all council information assets have a value and should be handled with care. As this is a broad category and there will be variety of handling instructions associated with this information, the Council is introducing sub-categories that give clear guidance on access arrangements for the information. These are:

OFFICIAL – PUBLIC – this is publicly available information or information where there is little or no damage if released
OFFICIAL – ALL STAFF – this is information that is widely available to all staff
OFFICIAL – RESTRICTED ACCESS – this is information where there is restricted access and a requirement for a 'need to know'
OFFICIAL – MEMBERS – this is information that is only available to all members/specific members
OFFICIAL – PRIVATE AND CONFIDENTIAL CORRESPONDENCE – this is emails/letters written to an individual containing their personal data

OFFICIAL–SENSITIVE – this caveat is used at the discretion of staff depending on the subject area, context and any statutory or regulatory requirements where it is **particularly important to enforce the need to know rules**.

Whilst the first four sub-categories have been adopted by Enfield Council to provide guidance to staff about handling requirements, the OFFICIAL-SENSITIVE caveat is an integral part of the government's classification scheme and will be recognised by the government and other statutory organisations as requiring additional measures of protection and distribution on a strict need to know basis.

OFFICIAL-SENSITIVE data cannot be shared externally except through an approved secure email system/secure network or appropriate data encryption and password protection and should be accompanied by a defined distribution list. Data sharing with external organisations must be in line with corporate data sharing agreements or contract terms.

The protective marking software is not available on the Council issued iPads at present.

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

19. Security of Equipment

Users are required to screen-lock their computers when moving away from their computer 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 bins' 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. Documents sent to a multi-function device (MFD) which incorporates follow-me printing can be collected using the appropriate identification card.

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

20. 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.

21. 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 the Council's Monitoring Officer 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.

22. 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.

23. 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 OFFICIAL – MEMBERS, OFFICIAL – RESTRICTED ACCESS or OFFICIAL - SENSITIVE, additional protections are expected.

I understand that I must maintain and safeguard the confidentiality of any and all sensitive information accessed or obtained in the performance of my authorized duties or activities. I will not access, use, and/or disclose OFFICIAL – MEMBERS, OFFICIAL – RESTRICTED ACCESS or OFFICIAL - SENSITIVE 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