Public Document Pack

Councillor Conduct Committee

Monday, 21 March 2016 at 6.30 pm
Room 3, Civic Centre, Silver Street, Enfield, EN1 3XA

Contact: Penelope Williams
Secretary
Direct : 020-8379- 4098
Tel: 020-8379-1000
Ext: 4098

E-mail: Penelope.Williams@enfield.gov.uk
Council website: www.enfield.gov.uk

Councillors: Claire Stewart (Chair), Elaine Hayward (Vice-Chair), Donald McGowan and Joanne Laban

Independent Persons: Christine Chamberlain and Sarah Jewell

AGENDA – PART 1

1. WELCOME AND APOLOGIES

2. SUBSTITUTIONS

Any member who wishes to appoint a substitute for this meeting must notify the Monitoring Officer in writing, before the beginning of the meeting, of the intended substitution.

Any notifications received will be reported at the meeting.

3. DECLARATION OF INTERESTS

Members are asked to declare any disclosable pecuniary, other pecuniary or non-pecuniary interests relating to any of the items on the agenda.

4. MEMBERS INFORMATION SECURITY POLICY (Pages 1 - 20)

To review the updated Members Information Security Policy.

To note that this item was postponed from the last meeting.

5. COUNCILLOR COMPLAINTS PROCEDURE (Pages 21 - 26)

To review the councillor complaints procedure. The current procedure is attached.

6. MEMBER/OFFICER PROTOCOL (Pages 27 - 42)

To review the Member/Officer protocol. The current Member/Officer protocol is attached.

7. REPORT BACK ON INDEPENDENT PERSONS TRAINING

To receive a verbal update from the Independent Persons on the training, recently attended.

8. UPDATE ON COUNCILLOR COMPLAINTS

To receive an update from the Monitoring Officer on councillor complaints received and currently being considered.

9. WORK PROGRAMME 2015/16 (Pages 43 - 46)

To note the work programme for 2015/16 and to consider the draft work programme for 2016/17.

10. MINUTES OF MEETING HELD ON 2 DECEMBER 2015 (Pages 47 - 50)

To receive and agree the minutes of the meeting held on 2 December 2015.

11. DATES OF FUTURE MEETINGS

To agree a date for an extra meeting of the Councillor Conduct Committee in order to enable the committee to consider a complaint against a councillor.

To note that dates for meetings in the 2016/17 municipal year will be agreed at the Annual Council meeting to be held on Wednesday 11 May 2016.

12. EXCLUSION OF PRESS AND PUBLIC

To pass a resolution under Section 100A(4) of the Local Government Act 1972 excluding the press and public from the meeting for any items of business moved to part 2 of the agenda on the grounds that they involve the likely disclosure of exempt information as defined in those paragraphs of Part 1 of Schedule 12A to the Act (as amended by the Local Government (Access to Information) (Variation) Order 2006).

There is no part 2 agenda.

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

This page is intentionally left blank

London Borough of Enfield

Procedure for Handling Complaints against Councillors and Co-opted Members

1. Introduction

1.1 The Council has established a Councillor Conduct Committee to implement the relevant requirements of Section 28 of the Localism Act 2011. These include arrangements for dealing with allegations that a councillor or co-opted member has failed to comply with the Authority's Code of Conduct.

1.2 The Councillor Conduct Committee comprises 4 members of the Council and deals with policy, complaints against councillors and issues concerning the members' Code of Conduct. The Localism Act also set up a role of Independent Person who will be consulted in respect of complaints received and before findings and sanctions are agreed. The Independent Person will not be a councillor and will be drawn from the local community. The Council has agreed to appoint two Independent Persons who will be recruited through public advertisement and a competitive interview process. Further information on the role of the Committee and the Independent Persons can be found at (insert hyper link)

1.3 Further reference to 'councillor' or 'member' in this document also refers to co-opted members of the Authority.

2. Key principles

The procedure for dealing with complaints should:

2.1 Be relevant to the Council's Code of Conduct

2.2 Have the confidence of the public, Council members and council staff.

2.3 Be as simple and economical as possible

2.4 Be speedy and fair to all parties

2.5 Be decisive

2.6 Provide oversight and support to the Monitoring Officer

2.7 Be proportionate and comply with the principles of natural justice

3. Criteria for eligibility of complaints

3.1 Complaints must be received by the Council's Monitoring Officer in writing within three months of the alleged matter, stating why it is felt the councillor concerned has breached the Code of Conduct. It will be considered solely on the evidence presented. The Council encourages complainants to provide their name and contact details. If the complainant asks for their identity to be protected, the Council will not disclose such details without their consent. The Council will not accept anonymous complaints. The Monitoring Officer will consult the Councillor Conduct Committee or relevant Independent Person as appropriate throughout the process – subject to neither being at risk of being compromised in the event of them being involved at some future point.

3.2 Complaints will not be accepted where:

(a) They are considered to be malicious, vexatious or frivolous

(b) The subject matter has already been considered by the Council - except where new evidence has become available which could not previously have been produced

(c) It would be more appropriate for the complaint to be dealt with by a court or under another complaints or arbitration procedure

(d) One of the parties had registered their intention to take legal action on all or some of the matters complained about

(e) Legal action is under way

(f) Some or all of the matters complained about have been resolved through litigation.

(g) The complaint is being/has been dealt with by another independent complaints process.

(h) The complainant seeks to overturn decisions made by the Council.

3.3 If a complaint is rejected on the basis of 3.2 above, there is no right of appeal.

4. Process

4.1 All complaints must be made using the Councillor Conduct Complaint Form attached as Appendix 1.

4.2 The Council will use its best endeavours to determine a complaint within 3 months of receipt. It will acknowledge the complaint within 5 working days, giving the complainant a contact name and details. The complainant will be kept informed of progress throughout. The process may include:

(a) Requests for further information/evidence

(b) Informal resolution to the satisfaction of all parties

(c) Mediation

(d) Investigation and/or

(e) Referral to the Councillor Conduct Committee where the Monitoring Officer feels it would not be appropriate for him/her to take a decision

4.3 The Monitoring Officer, based primarily on the criteria set out in paragraph 3.2 above, will consider the complaint received and, in consultation with an Independent Person, will determine whether it warrants further action.

4.4 If it is decided that the complaint does not warrant further action as it falls within the criteria in 3.2, the Monitoring Officer will advise the complainant accordingly with reasons.

4.5 If the complaint is referred for further action, the Monitoring Officer will determine, in consultation with the Independent Person, the most appropriate way of dealing with the complaint. The Monitoring Officer can either decide to determine the matter her/himself or refer it to the Councillor Conduct Committee.

5. Consideration of Complaints by Monitoring Officer

5.1 The Monitoring Officer may decide to undertake any investigation and other actions him/herself or appoint another person to act as investigating officer on his/her behalf. Whichever option is chosen, the outcome will be the responsibility (and in the name) of the Monitoring Officer.

5.2 Following an investigation which may involve requests for further information and advice, the Monitoring Officer or his/her representative will seek to resolve the matter to the satisfaction of all parties or carry out mediation.

(a) If the complaint is resolved, there will be no further action.

(b) If this is not possible the Monitoring Officer will either determine the matter her/himself or refer it to the Councillor Conduct Committee at this stage.

5.3 The Monitoring Officer will report quarterly to the Councillor Conduct Committee on:

(a) The number and nature of complaints received

(b) Those rejected with reasons

(c) Those resolved through informal resolution and other methods (eg mediation)

(d) The number investigated,

(e) Outcome/progress of investigations and action taken.

6. Appeals against Monitoring Officer decisions

6.1 In cases where the Monitoring Officer has either found no breach of the code or has determined the matter him/herself the complainant will have a right of appeal against this decision.

A councillor will also have a similar right of appeal against a Monitoring Officer decision.

6.2 Such appeals must be submitted on the template attached as Appendix 2 within 10 working days of the receipt of the decision.

6.4 Appeals under 6.1 above will be considered by the Councillor Conduct Committee, with advice from an Independent Person not previously involved, if available.

6.5 When considering the appeal the Councillor Conduct Committee will follow the procedure for appeal hearings (to be reviewed).

6.6 The attendance of the appellants will not be required unless the committee decides otherwise

6.7 If the Councillor Conduct Committee do uphold the appeal, and consider that there has been a breach of the code, they will have the option of considering further action, imposing sanctions or adjourning to seek further information.

6.8 There is no further right of appeal to the Council against the decision of the Councillor Conduct Committee. The decision made will be final and binding.

6.9 If the complainant feels that the Council has failed to deal with a complaint properly, and that this failure has caused injustice, a complaint can be taken to the Local Government Ombudsman.

7. Consideration of complaints by Councillor Conduct Committee

7.1 If appropriate, the Monitoring Officer (in consultation with the Independent Person) may refer the outcome of an investigation to the Councillor Conduct Committee.

7.2 The Committee will consider the Monitoring Officer/Investigating Officer's report which should include evidence and representations from both parties associated with the complaint. The attendance of the complainant(s) and the member(s) against whom the allegations were made will not be required, unless the Committee decides otherwise.

7.3 The Committee will follow the procedure for Councillor Conduct Committee hearings. (to be reviewed)

7.4 The Committee after considering the investigating officer's report will decide either that:

(a) The member concerned has breached the Code of Conduct; or

(b) There has been no breach

7.5 In the event of a finding of a breach of the Code, the Committee will have the option of recommending a sanction against the member concerned. This can include:

(a) Reporting the findings to full Council

(b) Recommending to the relevant Group Leader that the councillor be removed from relevant meetings of the Authority of which they are a member

(c) Recommending to the Leader of the Council that the member be removed from the Cabinet or from particular portfolio responsibilities

(d) Withdrawing facilities provided to the member by the Council – such as computer access and/or e mail or internet access

(e) Excluding the member from the Council's offices or other premises for a defined period of time – with the exception of meeting rooms as necessary for the purpose of attending meetings of the Authority of which they are a member

(f) Publishing the findings in the local media.

7.6 The decision will be communicated to all parties with reasons

7.7 Where there is a finding of no breach, the Committee will communicate the decision to all parties together with reasons.

8. Appeals against decisions of the Councillor Conduct Committee (in relation to 7 above).

The decision of the Councillor Conduct Committee will be final and binding with no further right of appeal to the Council. If the complainant feels that the Council has failed to deal with the complaint properly and that this failure has caused injustice, they can make a complaint to the Local Government Ombudsman.

This page is intentionally left blank

Chapter 5.5- Protocol for Member/Officer Relations

[Updated Council 29/01/14]

1. Introduction

1.1 This protocol is intended to guide members and officers of the Council in their working relations with each other. It is part of the Council's wish to uphold standards of conduct amongst councillors and officers.

1.2 A number of other documents also deal with standards of conduct for members and officers and lay down procedures for the proper conduct of Council business. These include:

- Local Government Act 2000
- Localism Act 2011
- The Council's Constitution, specifically:
    - The Code of Conduct for Members of the London Borough of Enfield (Section 5.1 of Part 5 of the Constitution)
    - The Code of Conduct for Officers (Section 5.4 of Part 5 of the Constitution).

For example, one of the general principles of the Code of Conduct for Members of the London Borough of Enfield states that…"(Members) should respect the impartial role of the authority's statutory officers and its other employees".

Equally, the Code of Conduct for Officers provides that Councillors should expect staff to contribute to proper and effective working relationships, to serve the Council as a whole, to maintain political neutrality at work and be seen to be impartial.

1.3 Councillors and officers are servants of the public and are indispensable to one another, albeit their responsibilities are distinct. Councillors are responsible to the electorate and serve only so long as their term of office lasts. Officers are responsible to the Council. Their job is to give advice to councillors and the Council, and to carry out the Council's work under its direction and control.

Mutual respect between councillors and officers is essential to good local government. However, over-close personal familiarity between individual councillors and officers can damage this relationship and prove embarrassing to other councillors and officers.

1.4 The protocol reflects the above principles, the Council's decision-making structure and the Local Government Act 2000 and Localism Act 2011 in relation to member conduct. It has also been written with the understanding that effective working relationships are required between councillors and officers to deliver the Council's objectives.

APPENDIX A

1.5 Whilst not covering every eventuality, it seeks to strengthen a good working relationship, to clarify possible areas of doubt and to offer advice as to how to deal with particular situations which might arise.

1.6 Whilst many of the situations which fall within this protocol will undoubtedly relate to councillors and senior officers, the same aspects of conduct apply to all employees.

2. Role of Councillors

2.1 All elected members have a right to professional, impartial and, if appropriate confidential advice from officers. They also have a right to expect officers to uphold and carry out the values of the Council and deliver policies within the agreed framework.

2.2 Councillors must abide by the Code of Conduct for Members of the London Borough of Enfield and the 10 principles that underpin this code, namely selflessness, integrity, objectivity, accountability, openness, honesty, leadership, respect for others, duty to uphold the law and stewardship.

2.3 They must declare any special relationships with constituents (ie spouse, partner, civil partner, family members or persons with whom they have a close association or personal relationship) when dealing with Council officers. Although members are elected to represent the interests of their constituents, they should not seek special treatment for any individual or themselves.

2.4 Without prejudice to their individual rights, all members shall have regard to the advice given by the Council's Monitoring Officer and the Councillor Conduct Committee in the exercise of their functions and duties, and they shall assist the Monitoring Officer in any aspect of investigations.

2.5 The law and the Council's Constitution lay down rules for the appointment, discipline and dismissal of staff. Councillors must ensure that they observe these rules scrupulously at all times. If councillors are called upon to take part in the appointment of an officer, the only question they should consider is which candidate would best serve the whole council. Section 7 of the Local Government & Housing Act 1989 requires every officer appointment to be made on merit. They should not let their political or personal preferences or prejudices influence their judgement. They should not canvass the support of their colleagues for any candidate and they should resist any attempt by others to canvass them. They should report any such attempt to the Chief Executive or the Monitoring Officer.

2.6 The recruitment and management of Council staff are the responsibility of the Chief Executive and the Council's Management Board. Except in cases where members are involved in the recruitment process as governed by the Officer Employment Procedure Rules, it is not appropriate for members to involve

themselves in these issues or to refer to such matters in public meetings or to the press (e.g. disciplinary cases).

2.7 Any act on the part of a member against an individual officer, if intended to gain unfair advantage or influence unfairly that person's actions, thoughts or deeds, may be regarded as a form of bullying, intimidation or harassment.

3. Officer Advice to Political Groups

3.1 There is now a statutory recognition for political groups and they are a well-established feature of local government. Officers may be called upon to give information and advice to party groups as part of the political consideration given to an issue before it reaches the formal decision making Council body. Political sensitivity and awareness are therefore required, particularly from senior officers. All members have the right to seek advice in confidence from senior officers, without it being perceived by others that the officer's political neutrality is being compromised. Whilst in practice such officer support is likely to be most in demand from the party group in control of the Council, it is an important principle that such support is available to all political groups.

3.2 Information may, from time to time, be requested by the Opposition Group from officers on a confidential basis. Providing this is not unlawful, improper, or against the interests of the Council specifically or generally, officers should respect the confidentiality of these discussions. If a councillor wishes such a discussion to be in confidence, he/she should state that to the officer at the outset. If the officer feels able to keep that confidence, then the discussion can proceed on that basis. If however the officer feels that it would not be in the best interests of the Council to keep the matter confidential, then he/she should say so at the time. The member concerned can then decide whether or not to proceed with the discussion.

3.3 Officers must be allowed to give support honestly but in a way that does not compromise their political neutrality. They also have a right to have their professional views listened to and respected (if appropriate in confidence) – but not necessarily followed – unless failure to do so would give rise to illegal, unlawful or improper conduct or maladministration. They should not be asked to make recommendations they could not professionally support. They should not be asked to justify political decisions of the administration or to be involved in advising on party business. Officers should ideally not be present at those parts of the meeting when such business is in fact discussed.

3.4 Advice and information given to party group meetings by officers is no substitute to them (the officers) providing all the necessary information and advice to the relevant decision making body of the Council at the appropriate time.

3.5 Members may ask officers to draft papers, resolutions or amendments to be presented to meetings. Whilst it is quite in order for officers to advise on such wording (e.g. to ensure legality or accuracy) this should not be taken that the officer supports the proposal.

3.6 Officers may be asked to give advice and information at meetings where non councillors are present. In most instances, such people (unless co-opted to a Council body) will not be bound by the Code of Conduct for Members of the London Borough of Enfield, particularly in relation to declarations of interest and confidentiality. Therefore in such circumstances, officers may not be able to provide the same level of information as they would for a member only meeting.

3.7 Exceptionally, Health and Wellbeing Board members (both councillors and non-councillors) are bound by the Code of Conduct for Members of the London Borough of Enfield. Board membership includes officers and councillors as well as other health and voluntary sector representatives. All are treated as co-opted members and are subject to the Code. Officers who are full Board members will therefore be subject to both the Code of Conduct for Members and the Code of Conduct for Officers.

3.8 Officers must respect the confidentiality of any party group meeting they attend.

3.9 Officers must abide by the terms of the Code of Conduct for Officers in relation to working with councillors.

3.10 Officers have a line management relationship with the Chief Executive or their Director – not individual members, whatever office that member might hold.

4. Officers' Roles

4.1 Employees serve the Council as a whole. They must have a loyalty to all councillors, not just those of any political group and ensure that the rights of all councillors are respected.

4.2 Officers must at all times keep members fully informed about significant issues which affect their wards or bodies on which they represent the authority. This is fundamental to the Council's wish to enhance the representational role of councillors. For example, if the authority conducts a consultation exercise in the borough, relevant members, including ward councillors should be notified at the beginning of the exercise.

5. Public Meetings called by Individual Councillors/Party Groups

5.1 Individual members or political groups may wish to hold public meetings, as part of their ward councillor role or in relation to a particular issue. Publicity for such

meetings should clearly state the nature of the event and should not imply that it is a Council meeting.

5.2 Any request for an officer to attend such a meeting in their official capacity must be made through the Chief Executive, their Chief Officer or the Monitoring Officer. It will be for those officers to decide if such attendance is both possible and appropriate, in the light of officer availability and priorities.

5.3 Any officer attending such a meeting does so in his/her official capacity. They are politically neutral and their presence does not imply support for a particular political proposal or initiative.

6. Public Meetings involving MPs, other Elected Representatives and Election Candidates

6.1 Where at any time an officer is invited to attend any public meeting called by or involving MPs, other elected representatives (e.g. GLA Assembly Members) or prospective candidates, such an invitation should be directed through the Chief Executive, appropriate Director or Monitoring Officer who will consult the Leader or relevant Cabinet member.

6.2 In the period between publication of Notice of Election (or Referendum) and polling day, the Council, its Members and its Officers must be aware of special rules designed to ensure the political impartiality of all Council publicity and communication. This period is generally known as “purdah” and will apply in the area in which the election or referendum is being held, whether that be the whole borough or one ward.

6.3 The Monitoring Officer will issue specific advice on purdah in the run up to any applicable electoral event, which will take the form of that set out at Appendix A.

6.4 If an officer is invited to attend any such public meeting in the purdah period, officers will only attend if representatives of all candidates standing in the election have been invited to the meeting. The same provisions apply in respect of local and national referendums.

7. Respect and Courtesy

7.1 For the effective conduct of Council business, there must be mutual respect and trust in all dealings between members and officers. As detailed in paragraph 12(2)(b) of the Code of Conduct for Members, members should not exert undue influence or inappropriately use their position in their dealings with officers. It is accepted that in some cases, discussions will be robust and challenging. Such dealings must however be conducted with courtesy, civility and professionalism, with respect for differing views and for legal and professional guidance. The way

in which members and officers work together will affect the external perception of the Council overall.

7.2 If a member feels that they have not been treated properly by an officer, they may take the matter up with the relevant Director. If the issue remains unresolved, they may raise it further with the Chief Executive or Monitoring Officer. A breach of the Officers' Code of Conduct could result in disciplinary action being taken against the employee concerned.

7.3 If an employee considers that they have been treated inappropriately by a councillor, they should raise the matter with their line manager or Director. The manager or Director will as appropriate discuss the matter with the member concerned or the party whip or group leader. If the matter directly relates to a group leader, the Chief Executive will be notified.

7.4 If the matter cannot be resolved it shall be referred to the Monitoring Officer who shall discuss the matter with at least one of the two independent persons to agree the most appropriate course of action within the Council's complaints procedure for Councillors.

8. Support Services to Members and Political Groups

8.1 The Council can only lawfully provide support services to members (e.g. stationery, typing, IT equipment, photo-copying etc) to assist them in carrying out their roles as councillors. Such support services must therefore only be used for Council business. They should never be used in conjunction with any party political campaigning activity or for private purposes unless with prior approval of the Monitoring Officer and full payment made to the Council.

9. Members' Access to Information and Council Documents

General

9.1 This part of the protocol should be read in conjunction with the Access to Information Rules in the Constitution and is without prejudice to rights members have to access information under the Freedom of Information Act 2000 and the Data Protection Act 1998.

9.2 Members have a right to request such information, explanation or advice, as they may reasonably need to assist them in carrying out their duties as a councillor. When information is requested on behalf of a third party, it must only be provided if it would be made available to a third party, on request under the Freedom of Information Act 2000.

9.3 The test to be applied in relation to a member's right to information or Council document is set out in common law and relates to a "need to know" to perform

their duties effectively as a councillor. Members do not have a right to a "roving commission" to examine documents – mere curiosity is not sufficient. The question of "need to know" must be determined initially by the Director who holds the document(s) in question. Councillors should not seek to obtain information where they have a Disclosable Pecuniary, personal or other pecuniary interest in the matter. In the event of dispute, the matter should be referred to the Council's Monitoring Officer.

9.4 For the purposes of this protocol, the term Council documents and information is applied very broadly and relates to that which is produced with Council resources. However, it should not be taken to include political documents / information.

9.5 Any information provided to a member must only be used for the purpose for which it was provided i.e. in connection with the proper performance of the councillor's duties.

9.6 Members are encouraged to use the Members Enquiry (MEQ) System, which is the most effective way to obtain appropriate information as efficiently as possible. Using the system also ensures that monitoring of service provision can be undertaken.

Meeting Documents

9.7 Members in law have a legal right to inspect any Council document, which contains information relating to the business to be transacted at a formal Council body. This right applies irrespective of whether the councillor requesting the information is a member of the body concerned and extends to background papers as well as reports to that meeting. The right does not however automatically apply to Part 2 papers as defined within the Local Government Act 1972 *(as amended)* as exempt and confidential information. According to the law, the member asking for the information would be expected to justify the request in specific terms, demonstrate a "need to know" in order to perform their duties as councillors which is not outweighed by any public interest requiring non disclosure, However in Enfield, the practice is to make Part 2 reports available to all members.

Documents in the possession/control of the Executive

9.8 Under the Local Government Act 2000, any relevant document in the possession of (or under the control of) the Executive and which contains material relating to any business to be transacted at a public meeting of the Council, will be available for inspection by any member of the Council. If the meeting is a private one *(where the relevant notice has been given)* any relevant document will be available for inspection **after** the meeting or immediately, in the case of Executive decisions by individual members or officers, after the decision has

been taken. In the case of documents containing exempt or confidential information the requirements in section 9.3 above will apply. In addition Members will not be entitled to access any document (or part of it) that would involve the disclosure of advice provided by a political assistant or adviser.

Scrutiny

9.9 In addition, and subject to important exceptions (see paragraph 9.9.4 below) an Overview and Scrutiny Committee member will be entitled to a copy of a relevant document which:

9.9.1 is in the possession or under the control of the Executive

9.9.2 contains material relating to:

9.9.2.1 any business carried out a private or public meeting of the Council or one of its decision making bodies;

9.9.2.2 any decision taken by a relevant Cabinet member in accordance with the Executive arrangements; or

9.9.2.3 any decision that has been made by an officer in accordance with the Executive arrangements.

9.9.3 The Executive will be required to provide a copy of the document as soon as reasonably practicable and in any case no later than 10 clear days after the Executive has received the request.

9.9.4 The exceptions are where the information:

(a) contains exempt or confidential information under the Local Government Act 1972, unless that information is relevant to:

- Any action or decision that the member is reviewing or scrutinising;
- Any review contained in the scrutiny work programme

(b) would involve the disclosure of advice provided by a political assistant or adviser.

9.9.5 If the Executive decides that a scrutiny member is not entitled (for the reasons above) to the information requested then it must provide the Overview & Scrutiny Committee with a written statement setting out its reasons for that decision.

10. Confidentiality of Information and Reports

APPENDIX A

10.1 The Chief Executive and Directors have a responsibility to ensure that all reports presented to formal Council bodies are only classified as “exempt” where the statutory criteria within the Access to Information Act are met.

10.2 In certain circumstances (known as Part 2 restrictions) the Council may restrict the circulation of documents in accordance with the exemptions within the Access to Information Act and where it is considered by the Chief Executive and the Monitoring Officer that such disclosure could be seriously detrimental to the Council’s interests, its employees or former employees, or that of a third party. The categories of information that might be restricted include:

10.2.1 Where any disclosure of information would be unlawful

10.2.2 Personal details of an employee, former employee or other third party

10.2.3 Details of a contract or property transaction

10.2.4 Legal or other officer advice in a contentious matter.

10.3 Members are reminded that they are supplied with Part 2 reports in their position of trust and must therefore not disclose that information – confidentiality must be respected. Any unauthorised disclosure of information could be a breach of councillor code of conduct.

10.4 The emphasis must be on producing as much information in the public part of the meeting as possible and restricting the “exempt information” to an absolute minimum. Where possible reports should be split between Part 1 (public session) and Part 2 (private session) so that only the minimum information is restricted.

10.5 Once a report has been issued as a Part 2 paper, and until such time as the relevant Council body or officer has had the opportunity to decide otherwise, councillors and officers must respect the confidentiality of the information. It is a betrayal of trust to breach such confidences. The wilful disclosure of such information by a member or an officer is likely therefore to be viewed as a breach of their respective codes of conduct.

10.6 The Council will respect the rights of members to access documents and information under the ‘need to know’ principle (see paragraph 9 above). However, members do not have an absolute right to every document. They must respect the confidentiality (where appropriate) of particular information in whatever form. To disclose information, knowing it to be confidential, is likely to be deemed a breach of the Councillors’ Code of Conduct.

10.7 In such cases, members may inspect the documents but not copy them. Arrangements for such inspection will be made by the Monitoring Officer at the time. The times during which members may inspect such documents will be as flexible as possible.

10.8 In addition Council has agreed separate arrangements for Cabinet in dealing with specific reports which deal with highly sensitive, exempt or confidential information, such as those identified in 10.2 above. These are referred to as "Super Part 2" but will only be used in exceptional circumstances (recognising members' statutory and common law rights). Under this procedure:

10.8.1 the Chief Executive (in consultation with the Monitoring Officer), relevant Directors and Cabinet Member(s) will agree the instances where it is felt the disclosure of particular information will be detrimental to the Council's interests, its employees or former employees and those of third parties;

10.8.2 circulation of any Super Part 2 report(s) will be restricted to Cabinet members, the statutory officers and relevant Director plus any members in attendance at the meeting. These copies will be numbered and collected in at the end of the relevant meeting.

10.8.3 there is a requirement for all members of Cabinet as well as the Leader of the Opposition Group (or nominated representative) to be briefed on the issue prior to its consideration by Cabinet along, when the issue has specific implications on their area, with relevant ward councillors.

10.9 The procedure recognises the additional rights given to members of scrutiny in terms of access to information so scrutiny members are able to request access to Super Part 2 reports, but only where clear reasons are provided and the issue is relevant to an issue under review or included on their scrutiny work programme. The Member concerned would need to understand and agree to respect the private and confidential element of the report and if appropriate may be asked to sign a confidentiality agreement. Where the decision on which a Super Part 2 report has been considered is subject to call-in, the chair of Overview & Scrutiny Committee must be briefed on the content of the Super Part 2 report in advance of the call-in meeting and a copy of the report tabled for all members present at the call-in meeting. These copies will be numbered and collected back when the call-in has been completed at that meeting.

10.10 The Chief Executive and the Monitoring Officer have an overriding duty to ensure compliance with 10.1 – 10.9 above.

11 Correspondence

11.1 In all cases, the Council's information governance protocols and obligations under the Data Protection Act 1998 must be observed.

11.2 Correspondence between an individual councillor and an officer should not normally be copied elsewhere without the knowledge of both parties.

11.3 Official letters on behalf of the Council should normally be sent out in the name of the appropriate officer, rather than a member. This is particularly important if the letter creates obligations or gives instructions on behalf of the Council. It may be appropriate in certain circumstances (e.g. representations to Central Government) for a letter to be sent signed by a member (e.g. Leader of the Council), but this should be the exception rather than the rule.

12 Relationship between the Mayor and Officers

12.1 The Mayor is the first citizen of the Borough. His/her role is to be an ambassador for the authority and to chair the Council meetings. Officers must give every support to the Mayor in the execution of these duties. However, the Mayor does not have any executive powers.

13 Relationship between the Leader of the Council, the Executive and Officers

13.1 Whilst the Leader and individual Cabinet members have executive powers, it is essential that they recognise and acknowledge that officers are required to serve the whole Council. On the other hand, it should be accepted that officers have a duty to implement the policies and decisions of the administration. They will have to give professional advice that might, at times, be unpalatable to the majority or minority group or individual councillors, but is felt to be in the best interests of the Council.

14 Relationship between Overview and Scrutiny and Executive Members and Officers

14.1 The Overview and Scrutiny function has within the Council's Constitution statutory rights with regard to access to information, member and officer attendance at its meetings, its role with Cabinet and conflict resolution direct to full Council. This is necessary to preserve its independence and role.

14.2 However the Overview and Scrutiny Committee has a responsibility to act reasonably and within the Constitution. The Monitoring Officer must be consulted if there are any doubts as to the legality of an Executive decision, or if it is felt that such a decision might be contrary to the Council's policy framework.

14.3 When calling Cabinet members, officers or other witnesses to give evidence at a scrutiny meeting, questions should be appropriate to their role. For example,

questions to officers should be confined to matters of fact and explanation of any professional opinion relating to policies and decisions. Officers must however respond to questions in an open, constructive and helpful manner. Any question relating to the justification of the policies or decisions should be directed to the relevant Cabinet member. Furthermore, Scrutiny members should not ask officers questions on issues that they know to be confidential.

14.4 The relevant chair of the scrutiny meeting must ensure that those giving evidence are not questioned in such a manner as could be considered by any reasonable person to be hostile, offensive, derogatory, harassing, bullying, victimising, discriminatory or otherwise unacceptable behaviour by a member. Chairmen also have a responsibility to ensure that members of the public are not allowed to disrupt the meeting or act in an aggressive or intimidatory manner.

14.5 Any allegations in relation 14.4 above should be referred to the Council's Monitoring Officer or to the Leader of the relevant political group.

15 Other Public Meetings

15.1 The same rules of behaviour in relation to scrutiny meetings apply to all other public meetings conducted by the Council e.g. Ward Forums – see paragraph 14 above.

APPENDIX A

Advice on "Purdah"

In order to maintain principles of good governance and to avoid unnecessary conflict with the issues of contention at an election or referendum (i.e. a "relevant issue"), basic adherence to the general rules of purdah will apply.

This note sets out some key information which you may find helpful and forms the basis of that which will be issued prior to relevant electoral events in the Borough by the Monitoring Officer.

General Information

In the period from publication of the statutory notice of election to close of poll at 10:00pm on polling day, the Council, its Members and its Officers should be aware of the special rules designed to ensure the political impartiality of all Council publicity.

Section 6 of the Local Government Act 1986 defines "publicity" as "any communication, in whatever form, addressed to the public at large or to a section of the public". This will include the obvious forms such as newsletters, magazines, press releases, posters and leaflets issued by the Council. It also includes the Enfield website, public meetings, local consultation exercises, exhibitions sponsored by the Council and press advertising, and can include spoken words addressed to the public or broadcast through radio, television or the Internet.

Generally, the Council must avoid:
• proactive publicity of candidates and other politicians involved directly in the electoral event;
• publicity that deals with controversial issues that could specifically be linked to a relevant issue (where this cannot be avoided, the publicity should present issues clearly and fairly with opposing points of views represented); and
• publicity that reports views, proposals or recommendations in such a way that identifies them with individual Members or groups of Members directly involved in the electoral event.

However the Council can:
• respond to events and legitimate service enquiries provided that the answers given are factual and not political; and
• comment on a relevant issue where there is a genuine need for a Member-level response to an important event outside of the Council's control.

Generally this means that during the election period the Council will:
• exclude all quotes from, and photographs of, Members directly involved in the electoral event in press releases, publications and other published material;
• refrain from organising photo opportunities or events which could be seen as giving candidates, Members or other political office holders directly involved in

the electoral event a platform for political comment;
• postpone publications, events or promotions until after the election if proceeding could give the appearance of seeking to affect support for a political party or candidate directly involved in the electoral event;
• not comment on matters of political controversy unless to refrain from comment would be harmful to the Council's best interests;
• avoid references in publications to the period the Administration has been in office or to the Council's future commitments if to do so could be seen to affect support for a political party or candidate directly involved in the electoral event;
• not undertake any other activity which could be seen as designed to benefit a particular political party or candidate directly involved in the electoral event.

The restrictions on publicity in an election period apply equally to publicity issued by third parties if they are assisted by Council funding. Where it could be shown that Council funding is being used to pay for, say, a charity's publicity, the Council will take reasonable steps to ensure that that organisation complies with the Code of Practice.

To be safe, the Council must plan to avoid publicity or public meetings about any locally controversial proposals or matters that could become an election or referendum issue. Events that could jeopardise our impartiality will be cancelled if they clash with the publicity restrictions during the pre-election period.

Public or committee meetings of a "business as usual" nature, unrelated to the election or referendum issues, may take place. This includes the determination of planning and licensing applications. However, everyone involved will be expected to observe the purdah constraints. The Monitoring Officer must be consulted in advance if there is any doubt as to whether a meeting might breach these guidelines.

If these rules about publicity are broken, the Council could be subject to legal challenge and, in a worst case scenario, election results could be invalidated. Officers who fail to observe the rules could be liable to disciplinary action.

Elected Members

Please note that the above restrictions generally relate to the Council and not to individual Councillors. This means that individual Councillors or political parties may contact the press directly, respond to their calls and set up their own photo shoots to promote a candidate or political party involved in the electoral event.

However, they may not use the Council's resources or facilities to do so. When at Council events, Councillors must not use that platform for political purposes. This includes Ward Forums, Overview and Scrutiny Committee and its workstreams and other public meetings.

In such circumstances, it is acceptable to include a note on political literature along the following lines:

“To contact your councillors about any matter for which the Council is responsible, phone _ (your Council funded line).

For any XXX party/election matter, please contact _ (political office number).”

Council Staff

Council staff should exercise extreme caution if invited to any event in which candidates in the election participate.

Managers of all Council-owned buildings should seek similar advice before allowing the Council's resources to be used for any “official or unofficial” visit by a candidate or political party directly involved in the election.

Schools

The Local Education Authority has a responsibility to ensure that its resources are not used for political purposes during an election period. Its employees also have personal responsibilities.

Head teachers and school staff should not be involved in any activity (in their official capacity) that promotes or is perceived to promote a political party or any candidate or politician involved in the election. This includes the endorsement of a candidate verbally or in writing. Some Head teachers and staff have been asked to do this in the past. They should, for example, refrain from photo opportunities with you, candidates or politicians or from participating in or organising events that could give others a platform for political comment or publicity.

Officers must not give support for one political party or candidate over others as such actions could leave them open to political bias and a potential breach of the Code of Practice.

Political parties may distribute leaflets outside of the school grounds providing they are not causing an obstruction or disturbance. They should not however enter the school premises.

APPENDIX A

Councillor Conduct Committee: Work Programme 2015/16

ITEM	Lead/ Support Officer	16 July 2015	17 September 2015	2 December 2015	24 March 2016
Annual Report	Asmat Hussain/Penelope Williams				**To agree Annual Report 2015/16 (taken forward to next meeting)**
Work Programme 2015/16	Asmat Hussain/ Penelope Williams	**To Agree the Outline Work Programme for 2015/16**	**Work Programme Monitoring**	**Work Programme Monitoring**	**Work Programme Monitoring**
Review of Code of Conduct and Complaints Processes	Asmat Hussain				**Review**
Update on Complaints Received	Asmat Hussain	**Update**	**Update**	**Update**	**Update**
Independent Persons Training	Independent Persons				**Report on training Received**
Complaints – Review of complaints received in 2015/16	Asmat Hussain				**Review of Complaints Procedure**
Member Training	Claire Johnson		**Update**		
Media Relations for Councillors	David Greely	**Report**			
Gifts and Hospitality	Asmat Hussain	**Report**			
Internet and Email Usage Policy for Councillors	Mohi Nowaz	**Report**		**Update**	**Update**
Review of Planning and Licensing Committees Code of Practice	Esther Hughes Andy Higham		**Report**	**Update**	
Regular update on Standards Matters – bringing members attention to recent standards news items for information.	Asmat Hussain	**If required**	**If required**	**If required**	**If required**
Review of Protocol for Member Officer Relations					**Report**
Review of Member's Expenses	Peter Stanyon			**Report**	
Dispensations		**Update**		**Revised form**	

This page is intentionally left blank

Councillor Conduct Committee: Work Programme 2016/17

ITEM	Lead/ Support Officer	July 2016	October 2016	December 2016	March 2017
Annual Report	Asmat Hussain/Penelope Williams				**To agree Annual Report 2016/17**
Work Programme 2016/17	Asmat Hussain/ Penelope Williams	**To Agree the Outline Work Programme for 2016/17**	**Work Programme Monitoring**	**Work Programme Monitoring**	**Work Programme Monitoring**
Review of Code of Conduct and Complaints Processes	Asmat Hussain	**Review**			
Update on Complaints Received	Asmat Hussain	**Update**	**Update**	**Update**	**Update**
Independent Persons Training	Independent Persons				**Report on training Received**
Complaints – Review of complaints received in 2015/16	Asmat Hussain	**Review**			
Member Training	Claire Johnson		**Update**		
Regular update on Standards Matters – bringing members attention to recent standards news items for information.	Asmat Hussain	**If required**	**If required**	**If required**	**If required**
Review of Protocol for Member Officer Relations	Asmat Hussain				**Report**
Review of Member's Expenses				**Report**	
Dispensations	Asmat Hussain	**Update**			
Gifts and Hospitality	Asmat Hussain				**Report**

This page is intentionally left blank

MINUTES OF THE MEETING OF THE COUNCILLOR CONDUCT COMMITTEE HELD ON WEDNESDAY, 2 DECEMBER 2015

COUNCILLORS

PRESENT Claire Stewart, Elaine Hayward, Donald McGowan and Joanne Laban, Christine Chamberlain (Independent Person) and Sarah Jewell (Independent Person)

OFFICERS: Asmat Hussain (Assistant Director Legal and Governance), Ellie Green (Trading Standards) and Andy Higham (Head of Development Management) Penelope Williams (Secretary)

306
WELCOME AND APOLOGIES

The Chair welcomed everyone to the meeting. Apologies for lateness were received from Councillor McGowan and Christine Chamberlain.

307
SUBSTITUTE MEMBERS

There were no substitute members.

308
DECLARATION OF INTERESTS

There were no declarations of interest.

309
CHANGE IN THE ORDER OF THE AGENDA

Members agreed to change the order in which items were considered on the agenda. Item 6 was taken before item 4. The minutes reflect the order of the original agenda.

310
DISPENSATION FORM

The Committee received a draft form for the recording of dispensations.

NOTED

1. The adoption of the form for recording dispensations would formalise the process and enable a more uniformed approach to be taken.

2. Dispensations are reported to the committee annually.

3. Four years is the maximum period for a dispensation to remain in place.

4. Space for a reference number would be included to the form.

5. The form will be added to the Members Portal.

AGREED that the form with the above amendment would be used for recording all dispensations in future.

311
MEMBERS INFORMATION SECURITY POLICY

This item was postponed for discussion at the next meeting.

312
PLANNING AND LICENSING CODES OF CONDUCT

The Committee received reports on the Planning and Licensing Codes of Conduct.

NOTED

1. Ellie Green, Principal Trading Standards Officer, reported that the Licensing and Gambling Code of Conduct had been revised, looking at the Councillors' main Code of Conduct and Planning Code, removing duplication, and using Plain English.

2. Andy Higham, Head of Development Management, reported that he had streamlined the Planning Code of Practice in a similar way.

3. The possibility of merging both codes had been considered but it had been decided that it would be better to keep them separate to avoid confusion about the different roles. Although there were some similarities most of the information within each code was only relevant to that area.

4. All new members of the planning committee receive training when taking up their new positions. Other regular sessions were held throughout the year. A record was kept. Information about the training available including a yearly schedule could be included within the Planning Code of Practice. Sessions open to all members could also be held.

5. Further refinements would be made taking account of the comments made at the meeting. The revised codes would be circulated to committee members for further comment before being sent for consideration at the Member and Democratic Services Group.

AGREED to note the proposed changes to the Planning Code of Practice and the Licensing Code of Conduct.

313
REVIEW OF MEMBER EXPENSES

The Committee received a report on members expenses outlining the expenses paid to members in pursuance of their duties and provides some comparator information.

NOTED

1. The information on expenses listed in the appendices covers the financial, rather than the municipal year.

2. Enfield has a similar level of expenses to comparator authorities.

3. Expenses information in the report is already in the public domain.

4. More details were requested on Councillor Goddard's 2013/14 expenses.

AGREED to note the information in the report.

314
UPDATE ON COUNCILLOR COMPLAINTS

Asmat Hussain, Monitoring Officer updated the committee on the complaints currently under consideration.

- Two complaints had been received which had both been discussed with Christine Chamberlain, Independent Person.

- Both had been accepted as valid complaints and were being referred for independent investigation.

- If a committee hearing is required to consider the complaints, a date will be found towards the end of January 2016.

315
MINUTES OF MEETING HELD ON 17 SEPTEMBER 2015

The minutes of the meeting were received and agreed as a correct record.

316
WORK PROGRAMME 2015/16

The Committee received and noted the updated work programme.

317

DATES OF FUTURE MEETINGS

The Committee noted the date agreed for the next meeting:

- Thursday 24 March 2015.