**E-mail, Internet & Social Networking Policy and Procedures**



Contents:

Introduction …………………………………………………………………. Page 3

Application ………………………………………………………………….. Page 3

Statement of Intent ………………………………………………………… Page 4

Standard of use for email, internet and Lync…………………………… Page 4

Use of E-mail and Lync ………………………………………………….. Page 5

Secure E-mail ……………………………………………………………….. Page 7

Personal Use of E-mail …………………………………………………….. Page 8

Use of the Internet …………………………………………………………... Page 8

Personal Use Internet .. …………………………………………………….. Page 9

Use of Social Media at Work ………………………………………………. Page 10

Use of Social Media Away from the Workplace …………………………. Page 11

Use of Social Networking Sites for Personal Use .………………………. Page 11

Monitoring of Internet Access at Work …………………………………….. Page 12

Open Access PCs for Internet Use ………………………………………… Page 13

|  |
| --- |
| **1. Introduction:**  |

E-mail and Internet are essential business tools for communication, obtaining and sharing information where this can save time and expense. This use includes viewing and creating content on ‘social media’ sites (e.g. Facebook, Twitter) which are accessed via the Internet.

Employees must follow the rules within this policy and procedure. It is a term of each employee's contract that he/she complies with these rules, and any breaches could lead to dismissal. You should also be aware that improper use of e-mail or the Internet could result in either you and/or the Council incurring civil or criminal liability. The Council also reserves the right to report any illegal activities to the appropriate authorities.

All the Council’s resources, including computers, personal handheld devices, e-mail and voicemail are provided for business purposes. At any time and without prior notice, the Council maintains the right and ability to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner, may be subject to scrutiny by the Council. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems. In order to ensure compliance with this policy, the Council may employ monitoring software to check on the use and content of any Internet access, Lync use or e-mail use, to ensure that there are no serious breaches of the policy. The Council specifically reserves the right for authorised personnel to analyse a users Internet Access Log and to access, retrieve, read and delete any communication that is created on, received through or sent in the email system, to assure compliance with all Council policies. Such monitoring will be used for legitimate purposes only.

Technology and the law change regularly and this policy will be updated to account for changes as and when necessary. Employees will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

Staff must abide by all of the Council’s Information Security Policies as published on Enfield Eye.

|  |
| --- |
| **2. Application:**  |

This policy applies to all employees, contractors, consultants, agency workers, casual workers and relief workers with access to e-mail, Lync and the internet, with the exception of school-based staff who, under local management arrangements are covered by procedures adopted by the Governing Body of each school.

Any reference to employee or staff shall for the purposes of this policy include contractors, consultants, agency workers, casual workers and relief workers.

This policy applies regardless of work location and therefore includes those working from home and includes personal online activity away from the workplace or use of personal resources

|  |
| --- |
| **3. Statement of Intent:** |

The aim of this policy is to be helpful, and to set guidelines on the use of e-mail, Lync, the Internet and social networking sites at work for the smooth and efficient running of Council business.

All new starters should be given a copy of this policy to read on the first day of their induction into the Council.

Self-employed contractors, agency workers or any other individuals working temporarily in the Council should be made aware of the rules regarding the use of e-mail, the Lync, the Internet and social networking sites. Breaches of this policy by contractors, agency workers or any other individuals working temporarily in the Council may result in the termination of their engagement.

These rules are designed to minimise the legal risks to the Council when employees and workers use e-mail and Lync at work and access the Internet. Furthermore, it aims to prevent misuse of internet, Lync and emails; protect Council data, systems and equipment; and encourage usage that supports the business goals and objectives of the Council. Where something is not specifically covered in this policy, employees should seek advice from their manager.

**4. Standard of use for Email, the Internet, Lync (inc Instant Messaging and Video Calls) and Social Media:**

You should not engage in any activity that is illegal, distasteful or likely to have negative repercussions for the Council, whether using Council systems or your own ICT resources which are linked to Council ICT systems. You must not upload, download, use, retain or distribute any images, text or software which:

* Includes offensive, threatening, illegal or obscene content of any sort. Material accessed involving child pornography and similar material will always be notified to the Police.
* Discriminates or encourages discrimination on the grounds of race, ethnicity,

gender, sexual orientation, marital status, disability or political or religious beliefs

* Involves distributing chain mail, including jokes, hoaxes or photographs.
* Knowingly uses material that infringes copyright or other intellectual property

rights.

* Misrepresents any matter to a third party or commits the Council to a legally

binding contract you are not authorised to do.

* Divulges confidential, personal or sensitive information to a third party.
* Uses a colleague’s email account or password without senior management

permission.

* Involves activities outside the scope of your responsibilities – for example,

unauthorised selling/advertising of goods and services.

* Involves activities that might affect the performance of or damages the Council’s system or network.
* Involves activities that might be defamatory or incur liability on the part of the Council or adversely impact on the image of the Council.
* Would be a breach of copyright or licence provision with respect to both programs and data.

The above is not an exhaustive or exclusive list of inappropriate usage.

The following activities are expressly forbidden:

* The wilful introduction of any form of computer virus.
* Seeking to gain access to restricted areas of the network or other hacking activities.
* Forgery.
* Attempts to read other users e-mail/Lync conversations without the relevant senior management

permission.

|  |
| --- |
| **5. Use of E-mail and Lync (inc Instant Messaging and Video Calls):** |

**Contents of E-mail, Instant Messages (IM) and Video Calls (VC)**

E-mails and IMs that employees intend to send should be checked carefully. They should be treated like any other form of communication and, as such, what is normally regarded as unacceptable in, for example, a letter is equally unacceptable in an e-mail and IM. VCs should only be used for business purposes. All emails, IMs and VMs are recorded and can be viewed by the Council even after an employee deletes them from their account.

Employees must not use the Council’s facilities to send or solicit an e-mail where the content (or any attachment) is pornographic, sexist, racist, homophobic, of a sexual nature or innuendo, or defamatory or in any way breaches the [Employee Code of Conduct](https://enfield365.sharepoint.com/%3Aw%3A/s/intranethr/ETWgqeGxwNxOgkimwwEMGzcBAK_j8guXb4esutLdeiUTMw?e=3HdEKa) or [Equality in Employment Policy](https://enfield365.sharepoint.com/%3Aw%3A/s/intranethr/Efxnwg_TSlpPl98jQ45sungBDbB5osCqpj8kjD1RTKExUA?e=07Twm8) (this applies to both business and personal use). Employees must not make statements on their own behalf, or on behalf of the Council, which are or may be defamatory or damage the reputation of any person, or bring the Council into disrepute.

The use of e-mail, IM and VC to send or forward messages, which are defamatory, obscene or otherwise inappropriate, will be treated as misconduct under the Council’s [Principles of Managing Misconduct](https://enfield365.sharepoint.com/%3Aw%3A/s/intranethr/EV9hBq5sCoBKqHER4A6NAYkBjb3h2IxHzuL3wtjTTv9JiQ?e=lUMJhq). In serious cases this could be regarded as gross misconduct and may lead to dismissal.

E-mails, IM and VC that have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating, receiving or forwarding any offending material can be identified. Offending material, both in hard copy and electronic form, may be admissible in a court of law.

Equally, if an employee receives an obscene or defamatory e-mail, IM and VC whether unwittingly or otherwise and from whatever source, he/she should **not** forward it to any other internal or external e-mail address. If an employee receives an email, IM and VC that they believe to be of this nature, they should report this to their line manager.

Staff must **not** use their e-mail facility to conduct a business.

Unauthorised use of another user’s password or mailbox is prohibited.

Employees must not send ‘all Enfield’ e-mails unless they have the specific authority of a Director or an Assistant Director who has the appropriate authority from a Director.

Employees must retain/archive e-mails in accordance with Enfield Council’s Information Retention Policy

All Council employees who require access to GCSx e-mail must read, understand, and sign the GCSx Personal Commitment Statement.

**Corporate information to be included in e-mails**

Employees should ensure that official corporate information is given as a signature on any e-mails that they send externally.

An example of the e-mail layout is provided below:

John Smith

IT Manager

London Borough of Enfield Council

Tel (+44) (1) 11 1111 111

Mobile (00000 000000)

Fax (+44) (1) 11 1111 111

John.Smith@enfield.gov.uk

Enfield Council is committed to serving the whole borough fairly, delivering excellent services and building strong communities.

**Copying e-mail to others**

Employees should exercise care not to copy e-mails automatically to all those copied in to the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person.

**Attachments**

Before sending an attachment via e-mail, IM or VC employees should be confident that the attachment does not contain a virus. The Council could be liable to the recipient for loss suffered. The Council has virus-checking in place but, if in doubt, employees should check with the IT department.

Employees should exercise extreme care when receiving e-mails or IM with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

|  |
| --- |
| **6. Secure E-mail:**  |

Instructions for the use of secure e-mail are contained within the Secure E-mail Policy.

|  |
| --- |
| **7. Personal use of E-mail, IM and VC:** |

The e-mail and Lync is for Council business use only. However the Council understands that employees may on occasion need to send or receive personal e-mails using their work address or using Lync. Employees wishing to send or receive personal messages are permitted to do so on an occasional basis, preferably outside working hours or during official breaks, and so long as it does not impact on day to day work. Managers should note that there might be times when an employee receives a personal e-mail unexpectedly.

Employees who abuse the e-mail or Lync for personal use or to operate a business with be dealt with accordance with the Council’s [Principles of Managing Misconduct.](https://enfield365.sharepoint.com/%3Aw%3A/s/intranethr/EV9hBq5sCoBKqHER4A6NAYkBjb3h2IxHzuL3wtjTTv9JiQ?e=lUMJhq)  For the sake of clarification a type of activity that may constitute abuse of the systems is high volume of outgoing and incoming personal e-mails or Lync conversations. High volume is determined solely by the manager. Excessive use of personal smartphones, tablet computers etc. during work time to access the internet and social media may also lead to disciplinary action.

The Council reserves the right to monitor employees' e-mails. The Council may check email accounts during periods of employee absence, if the Council suspects inappropriate use (eg material containing sexist, homophobic, racist terminology, nudity or other inappropriate content (although the Council understands that it is possible for employees to inadvertently receive such material and they will have the opportunity to explain if this is the case)), if the Council suspect excessive personal use and/or if the Council suspects the employee is sending or receiving emails that are detrimental to the Council, or any other substantial reason.

|  |
| --- |
| **8. Use of the Internet:** |

This policy covers all electronic devices supplied by the Council, which permit access to the Internet and includes viewing and creating content on web-based social media services such as Facebook and Twitter. It also applies to personal online activity away from the workplace using personal ICT resources, where this may bring the Council into disrepute

You must:

* Be aware that leaving your email address on internet sites may lead to you

receiving unsolicited emails.

You must not:

* Access, download, forward, publish, store (on any storage medium) or print internet sites which contain offensive, sensitive, malicious or illegal material of any sort e.g. pornography, racist or sexist material, or violent images or which brings the Council in to disrepute.
* Access or place any material on the Internet that might be considered

inappropriate or offensive to others.

* Use the Internet for personal gain or profit, including share dealing or gambling.
* Conduct online financial transactions as part of a private business for gain.
* Download or store materials from the Internet for non-work purposes.
* Copy software files from the internet – this is not permitted. Software downloads must only be carried out by authorised ICT staff.
* Access any sites or download or print any files displaying material, which the user knows to contravene the Council’s Equality and Diversity policies (including any Codes of Practice covering discrimination/bullying). If such a site is accessed inadvertently, the user’s line manager should be informed immediately.
* Respond to surveys on the Internet on behalf of the Council without consulting your line manager.
* Open a subscription account on the Internet on behalf of the Council without consulting your line manager.
* Access the Internet unless it is under your own username and password.
* Leave your computer unattended whilst logged on to the Internet.

Examples of inappropriate downloading includes any software (freeware or shareware) or information from external or internal sources that potentially breaches copyright law or intellectual property law including fonts, games, screensavers, desktop wallpaper, video clips, photographs/pictures and music files. This is not an exhaustive or exclusive list of inappropriate usage of downloading.

Do not download any information that can lead to criminal prosecution e.g. pornography, sexist or racist material, and incitement to religious hatred or advocating violence to a particular group. This also includes any copyright materials such as screensavers and music as mentioned above. As a safeguard against fraud, you should never provide personal data of any sort. Information (such as credit card details) sent across the Internet, can be “stolen”, read or altered, unless encrypted. Do not send details on the Council’s behalf unless the Internet site has a certificate of encryption and you are authorised to do so.

Remember – you are responsible for all internet sites accessed under your login. The

Council can monitor your Internet usage – the internet sites you visit at work are recorded. Employees may be called upon to justify the amount of time they have spent on the Internet or the sites that they have visited. Material accessed involving child pornography and similar material will always be notified to the Police.

**Licenses and Contracts**

Some websites require the Council to enter into licence or contract terms. The terms should be printed off and sent for approval in advance or e-mailed to Legal Services department **before** an employee agrees to them on the Council's behalf. Employees should, however, always consider whether the information is from a reputable source and is likely to be accurate and kept up to date, as most such contract terms will exclude liability for accuracy of free information.

Employees should download work related files on to only those PCs with virus checking software and should check how long the download will take. If there is any uncertainty as to whether the software is virus-free or whether the time the download will take is reasonable, the relevant line manager and the Council's IT department should be consulted.

Employees are **not** permitted to download or store files or software for personal use, for example, music or pictures.

**Removing Internet Access**

The Council reserves the right to deny Internet access to any employee at work, although in such a case it will endeavour to give reasons for doing so.

**Registering on Websites**

Many sites that could be useful for the Council require registration. Employees wishing to register as a user of a website for work purposes are encouraged to do so. However, they should ask their manager for permission before doing this.

**Prohibited use of the Internet**

Abuse of Internet access is inappropriate behaviour for which individuals will be subject to disciplinary action and possible criminal prosecution depending on the nature of the offence. The following are examples, which could constitute gross misconduct and can result in summary dismissal, (these examples are neither exhaustive nor exclusive).

**Inadvertent use of the Internet**

It is recognised by the Council that staff may, during acceptable use of the Internet, make inadvertent access to a site or page that contains material which is unlawful, indecent or objectionable. In this circumstance, the individual should disconnect from the internet immediately and notify their line manager as soon as possible after the incident, providing details of the date and time of the inadvertent access. The ICT Helpdesk should also be advised (in writing) so that steps may be taken to block any further access. Do not forward on any material inadvertently accessed.

|  |
| --- |
| **9. Personal use of the Internet**  |

The Council provides access to the Internet as a business tool. However, it is accepted that employees may use these facilities for limited personal use. This must normally be restricted to outside working hours or during your official breaks. Permitted personal use is, of course, subject to the restrictions as set out in this guidance and must not impact on your day to day work.

If you know or suspect that someone is breaching this policy / guidelines, the Council would expect you to raise your concerns at the earliest opportunity. You can do this by:

* Informing your line manager,
* Contacting the Chief ICT Officer.
* Contacting the Chief HR Officer or Chief Auditor under the Council’s Whistle

blowing Policy.

Any breach of this policy will be dealt with, where applicable, in line with the Council’s Principles of Managing Misconduct.

|  |
| --- |
| **10. Use of Social Media at Work:** |

Access is permitted to some social media sites such as Facebook and Twitter and YouTube via the Council’s email and internet systems. Access is normally authorised for the purposes of conducting Council business. Specific guidance is available on the professional use of social media for communications, customer service and public engagement on behalf of the Council.

In general, access to social media sites, chat rooms, bulletin boards, newsgroups or any similar Internet service at work should mainly relate to Council business. However, it is accepted that employees may use these facilities for limited personal use. This must normally be restricted to outside working hours or during your official breaks. Permitted personal use is, of course, subject to the restrictions as set out in this guidance and must not impact on your day to day work.

Excessive and repeated use of personal smartphones, tablet computers etc. during work time to access the internet and social media may lead to disciplinary action. Anyone using social media services should consider the level of privacy they are comfortable with, and to restrict access to their personal information accordingly. Employees are reminded that material posted on social media sites may be viewed by people who were not the intended recipients. Some people prefer to keep their work and personal lives separate so careful thought should be given to including work colleagues in social media networks e.g. as Facebook ‘friends’. Staff posting content on professional social media sites, blogs etc. should state they are doing so in a personal capacity, and even then be mindful of saying things that could embarrass the Council.

Under the Employee Code of Conduct, there are some political restrictions placed on certain post-holders by the Local Government and Housing Act 1989 and ensuing Regulations, and those political restrictions should be considered when posting content online.

|  |
| --- |
| **11. Use of Social Media Away from the Workplace:** |

The Council recognises that many employees make use of social media in a personal capacity, away from work and in their own time. This is their own personal business as they are not acting on behalf of the Council. However employees must be aware that they can damage the Council’s reputation if they are associated with damaging content and identified – deliberately or inadvertently - as a Council employee.

Staff should take reasonable steps to keep their work and personal profiles separate. For instance, your online profile (for example, the name of a blog or a Twitter name) must not contain the name of the Council and you must not use the Council logo to brand your blog or personal website. Any communications that you make in a personal capacity through social media must not bring the Council into disrepute by breaching confidentiality and/or do anything that compromises an individual’s adherence to the Code of Conduct at work. Even if a personal profile appears private, any information that is posted on social media platforms can potentially end up on the WWW public domain.

Any breach of this will be dealt with, where applicable, in line with the Council’s Principles of Managing Misconduct.

|  |
| --- |
| **12. Use of Social Networking Sites for Personal Use**  |

Where an employee uses non-Council computer equipment in their free time to connect to the internet and create or use social networking sites in a personal or private capacity, they must adhere to the following:

* Employees must be personally responsible for everything on their personal pages including any link to any material on other web pages.
* The Council’s logo must not be used on any personal page.
* Employees must not claim to be representing the Council when using social networking sites in a personal capacity.
* Employees should be mindful that stating they are employed by the Council does not infer ‘representation’ of the Council.
* Employees should understand their online privacy settings – check the settings and understand who can see the information published and personal information.
* All employees should be aware of and follow the Staff Information Security Policy
* If an employee does talk about the work they do or an Enfield Council service they are associated with, they must make it clear that they are speaking for themselves and not on behalf of the Council. Use a disclaimer such as: “The views expressed here are my own and do not necessarily represent the views of Enfield Council.”
* Employees must not let the use of social networking interfere with their job and always access in their own time as detailed above.

When using social networking sites for either business or personal purposes employees must not:

* use the Council’s logo, official or otherwise, without the specific written consent of the Director of the department
* write about their work or make reference to the Council on external web pages, i.e. in blogs or on social networking sites, when using the sites for personal purposes
* disclose any information that is confidential to the Council or any third party or disclose personal data or information about any individual/colleague/service user, which could be in breach of the Data Protection Act or Information Security requirements
* disclose any information, which is not yet in the public arena
* post illegal material, e.g. images of child abuse or material which incites racial

hatred

* link their own blogs/personal web pages to the Council’s website
* include any information, sourced from the Council, which breaches copyright
* make defamatory remarks about the Council, colleagues or service users
* publish any material or comment that could undermine public confidence in you as an employee/officer of the Council and/or in position of trust within the community
* misrepresent the Council, by posting false or inaccurate statements about the work of the Council.

|  |
| --- |
| This list is not exhaustive.Any breach of this policy will be dealt with, where applicable, in line with the Council’s Principles of Managing Misconduct.  |
|

|  |
| --- |
| **13. Monitoring of Internet Access at Work:**  |

 |

The Council reserves the right to monitor employees' internet usage. The Council considers the following to be valid reasons for checking an employee's internet usage:

* If the Council suspects that the employee has been viewing or sending offensive or illegal material, such as material containing sexist, homophobic, racist terminology, nudity or other inappropriate content (although the Council understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case);
* If the Council suspects that the employee has been viewing obscene or pornographic sites;
* If the Council suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.
* If the Council suspects that the employee has posted offensive or inappropriate comments or information that may undermine public confidence or damage the reputation of the Council or its partners.

This list is not exhaustive

|  |
| --- |
| **14. Open Access PCs for Internet Use:**  |

There are three computers in the Civic Centre canteen that can be used for personal use. They are free of charge to use, allowing employees and visitors to access their personal email (for example Yahoo mail) as well as social networking sites and online banking.

These PCs must not be locked and documents must not be saved to the desktop.

These PCs are not attached to the Council’s main network, and therefore have no restrictions to access; however access to offensive or illegal material, such as material containing homophobic, sexist or racist terminology or nudity is prohibited.

Any employee found accessing this material will be dealt in accordance with the Council’s [Principles of Managing Misconduct.](https://enfield365.sharepoint.com/%3Aw%3A/s/intranethr/EV9hBq5sCoBKqHER4A6NAYkBjb3h2IxHzuL3wtjTTv9JiQ?e=lUMJhq)