Acceptable use policy

Purpose and applicability

This policy defines the acceptable use of Enfield Council's information assets and those assets provided to the council by partner organisations. This includes the End User Computing and Smart Mobile Devices hardware and the information accessed by those devices. It is known as the 'Acceptable Use Policy' or 'AUP'.

This policy applies to council workforce including temporary and agency workers, volunteers, independent consultants and suppliers/contractors who need to use council information assets, as part of/to carry out their duties. These people are referred to as 'users' in the rest of this document. Note that there is a separate AUP for Members.

Acceptable use means that access to information is legitimate, it is used only for the intended purpose(s), the required standards of practice are in place to protect the confidentiality, integrity and availability of information, and the use complies with relevant legislation and regulation.

The council will at all times to conduct its business in a professional manner and to provide the highest possible level of service, both internally and to its customers. Any loss, compromise, or misuse of council information and associated assets, however caused, could have potentially devastating consequences for the council and may result in financial legal action.

LIVE CHAT

Definitions

An **information asset** is any data, device, or other component of the environment that

supports information-related activities. Assets include hardware (for example, laptops), software and confidential information (for example, a person's record).

Inappropriate use of information assets exposes the council and the service users who entrust us with their data to risks.

A **data subject** is a person or organisation to whom data relates.

A **data controller** is a person or organisation who is legally in charge of a data asset. The council is the data controller for many of the assets it holds.

A **data processor** is a person or organisation who is tasked by a data controller with using a data asset. The council is a data processor for some organisations such as the NHS and Police.

A **user** is any person or organisation accessing information assets.

Personal data is data that relate to an individual. For example, your name, address and date of birth are examples of your personal data.

Special Category personal data is data revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. This is commonly referred to, along with other data, such as financial information, as 'sensitive'.

'PC' means any computer device such as a tablet, laptop or desktop.

'Mobile' means any Smart Mobile Device that is portable with a mobile network voice or data connection, including smart phones, standard phones, tablets or portable devices such as printers and ticket reading devices. Note that some tablet devices (for example, a tablet with a mobile network connection) fall into both the PC and mobile category and rules for both must be followed.

'BYOD' Bring Your Own Device is the practice of allowing employees to use their own computers smartphones and other devices for work purposes.

Policy statements

It is the responsibility of all users to have annually read and know this policy and to conduct their activities accordingly. Breach by any user could result in disciplinary action or other appropriate action being taken.

Council information facilities are provided for business purposes only, with limited personal

use permitted as defined elsewhere in this document.

Use of information facilities must be authorised by line managers.

Any use of council facilities for unauthorised purposes may be regarded as improper use of facilities. Council IT systems must display an appropriate warning notice to this effect when users log on.

Users should be aware that any data they create on council systems (including anything pertaining to themselves) is deemed to be the property of council. Users are responsible for exercising good judgment regarding the reasonableness of personal use and to be compliant with the Employee Code of Conduct.

For security and network maintenance purposes, authorised users may monitor equipment, systems and network traffic at any time. The council reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact the Digital Services (DS) Service Desk.

This policy is supported by a number of other policies which should be read in conjunction with it.

Use of personal data

The council has access to a wide range of personal data entrusted to us by our citizens and others. This data must be used and access in accordance with law as defined by statutory GDPR.

Users must only use personal data in accordance with the agreed and published purposes for the collection of data. Using personal data in any manner requires a clear legal basis or consent from the Data Controller whether personal or corporate. Merging personal data with other sources, for example, is not permitted unless a legal basis or consent is present, and the use of the data correctly authorised.

Information system security

Security of the council's information assets is paramount. All information assets must be treated as confidential unless marked as public. The council is the data controller for most information assets held, however users must be aware that the council acts as a data processor for other organisations. Users with access to such information assets must

maintain awareness and compliance with the data owner's policies.

Security controls and reporting

The council has implemented security systems to safeguard information assets. These include controls over viruses, offensive and illegal material, disruption to our systems, and unauthorised access. Bypassing or attempting to bypass these security systems is a breach of policy.

To be effective, all users must support and use these systems and must assist in identifying and eliminating threats to information security. Any breach or suspected breach of this policy must be regarded as a security incident.

Users must report security incidents to the DS Service Desk immediately.

Use of downloaded programmes

Under no circumstances may users use any programme that is not already installed on a PC or download programmes from the Internet for use on council DS systems. For mobile devices, only pre-approved applications will be installed.

All smart mobile devices will be managed through the Mobile Device Manager. Attempts to breach this will be seen by the system.

Council applications and logins should not be downloaded onto personal smart mobile devices (BYOD).

For those who currently have this access (as at 01/01/2023) there will be a 6-month clemency window for this to be removed and transfer to the new council smart mobile devices.

Passwords

Users are responsible for the security of their passwords and accounts. Passwords must be kept confidential and not shared with others.

Passwords will be changed every 3 months and the system will prompt this change. Failure to change will cause the user account to be locked until the change is made. The reuse of old passwords is not permitted.

Temporary passwords must be changed at the first log on. Passwords must be changed whenever there is any indication of possible system or password compromise.

If legitimate access to an absent person's system or data is required, this can only be done by their line manager and then written or email authority must be provided by a senior manager of the users and approved by a Head of Service or Director.

All EUC or smart mobile devices accessing resources must be secured with a password protected screensaver with the automatic activation feature set at 2 minutes or less, if the device is inactive or unattended.

Internet usage

The Code of Conduct provides detailed guidance.

The council provides access to the information resources on the internet to help users carry out their functions. The provision of Internet access is at the council's discretion and users provided with internet access are required to read and adhere to this policy.

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

Email usage

Enfield Council email system is for council business use only. The use of Enfield Council email for personal business is forbidden.

However, the council understands that users may on occasion need to send or receive personal emails using their work address. Users wishing to send personal email to an alternative email address must seek the prior permission of their manager.

Auto forwarding of email to external email accounts (non LBE) is expressly forbidden.

All emails sent by users on council business should be spell checked before sending. In addition, it is not acceptable for the message to be abusive or out of context of the business in hand. Please note that wording should be full English wording and not shorthand text that might be used when texting on a mobile.

The sender of the email is responsible for the safe arrival of information at its intended destination, it should be noted that it is the sender who is usually liable for any breach of security and confidentiality.

Sending emails internally is secure. Sending emails externally is not generally secure and they can be intercepted and viewed by unauthorised people. Secure email must be used when

emailing information to external agencies or individuals when the content of the email 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 email address outside of Enfield Council, unless it is absolutely necessary and the transmission is secure. This can be done using:

- Microsoft Office 365 mail to government agencies (.gov.uk, .nhs.net).
- EFT System – see Secure File Transfer Guide.
- Microsoft Office 365 classification – all emails marked 'OFFICIAL – SENSITIVE' and sent externally are encrypted.

Staff must be vigilant with attachments to emails and links to documents downloaded from other locations as they may contain viruses. Users who suspect a possible virus attack must report it to the DS Service Desk immediately.

Staff must be aware that email is easy to forge and that attacks based on this are common. Always treat emails asking for unusual actions with suspicion. For example:

- any email asking to move money should be confirmed in person or by telephone
- any email asking for a password or to click on a link which then asks for username, password or bank details even if it appears to be from DS may be fake - DS will never ask for these details
- emails containing urgent invoices are likely to be fake - invoices should go via our scanning facility

For further information regarding secure information exchange (for example, via email and Cloud Storage) please refer to relevant policies including and not limited, ‘Data Protection Policy’ and ‘Information Classification and Handling Policy’.

Responding to security incidents and malfunctions

Any perceived or actual information security weakness or incident must be reported to the DS Service Desk immediately. Examples of a security incident include unauthorised access to information assets, misuse of information assets, loss/theft of information assets, virus attacks, denial of service attacks, suspicious activity.

Further information on the reporting of security incidents can be found in the Security Incident Reporting Procedure.

Computer viruses and other harmful code

End User computing devices, including PCs, laptops and networking devices are continually scanned for malicious activities and vulnerabilities. To support this process and allow quiet hour background processes to complete all users should shut down their devices at the end of the working day to allow updates to complete on restart.

Software applications used on council networks go through an extensive evaluation process before acceptance into the software catalogue and users wishing to use software applications not available within the existing software suite should approach DS for advice. Under no circumstances are users to attempt to download unvalidated software applications.

It is a crime under the Computer Misuse Act 1990 to deliberately introduce malicious programmes into the network or server (for example, viruses, worms, Trojan horses, email bombs). Users must not use council facilities for intentionally accessing or transmitting computer viruses or other damaging software or software designed for creating computer viruses.

If you are in doubt about any data received or suspect a virus has entered your PC, log out of the network immediately, stop using the PC and inform the DS Service Desk on the number at the top of this document.

All users should shut down their device at the end of each working day to ensure that the relevant updates are deployed to their machine.

Any user downloading a file or software from an external site should seek assistance from DS **before** downloading.

Hacking and associated activities or breaches of policy

It is a crime under the Computer Misuse Act 1990 to enter into another computer system without authorisation.

Council IT facilities must not be used in any way that breaks the law or breaches standards. Such actions could result in disciplinary action being taken.

Users must not use council facilities for:

- sending threatening, offensive or harassing messages
- creating or sending obscene material
- accessing or transmitting information about, or software designed for, breaking through

security controls on any system
- effecting security breaches or disruptions of network communication. These include, but are not limited to:
- accessing data to which the user is not an intended recipient without permission, even if it is not protected by security controls
- logging into a server or account that the user is not expressly authorised to access
- network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- port scanning or security scanning (unless prior authorisation has been granted)
- executing any form of network monitoring which will intercept data not intended for the user (unless prior authorisation has been granted)
- circumventing user authentication or security of any host, network or account
- interfering with or denying service to any user (for example, denial of service attack)
- using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's communication session, via any means, locally or via the Internet / Intranet / Extranet

Users may be exempted from the some of the above restrictions during the course of their legitimate job responsibilities (for example, systems administration employees may have a need to disable the network access of a host if that host is disrupting production services). Such exemptions should be included in an Access Matrix and approved and documented by the DS Security Manager.

Copyright and encryption

It is illegal to break copyright protection. Users could break copyright if they download, transmit or copy protected material.

Users must not:

- transmit copyright software from their PC or allow any other person to access it from their PC unless the controls/licence so permits
- knowingly download or transmit any protected information/material (including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources and copyrighted music) that was written by another person or organisation without getting permission
- copy/install copyright software from/to their PC for any purpose not approved by the licence and for which LBE or the user does not have an active licence
- transmit software, technical information, encryption software or technology, in violation of international or regional export control laws

The DS Security Manager should be consulted prior to export of any material that is in

question and all information in this respect should be documented accordingly.

Unattended user equipment

Users must not leave their workstation unattended without ensuring that sensitive information is not visible on their screen or screen saver has locked access.

All EUC or smart mobile devices accessing resources will be secured with a password protected screensaver with the automatic activation feature set at 2 minutes or less if the device is inactive or unattended.

Users accessing sensitive information whilst remote working must position their workstation in such a way that the information is not visible to unauthorised users or you must use privacy screen.

No paper copies of data, memory sticks or other portable media may be left on desks when unattended.

Lockable cabinets need to be available to store sensitive documentation when a desk is unattended.

Hardware usage

All council owned computer equipment and software remain the property of the council. Any user who leaves council employment / engagement is required to return all hardware and software that has been provided to them on or before their last day of employment as directed by their line manager.

Only hardware provided by the council is authorised for use for council business. Users must not attempt to attach any other equipment to council hardware or to network or telephone sockets.

BYOD or the use of personal computers, smartphones or other devices is prohibited for use.

Software usage

Enfield Council is committed to the use of authorised software within its computer systems. It is expressly forbidden for users to load or operate software gained from the Internet, magazines or other sources. The council is also committed to using software for which it has current licences.

It is the responsibility of all users to ensure that they do not introduce viruses into computer

systems. Users should take care when receiving electronic information from unknown sources, including attachments within email. Where there are reasons to access information from questionable source(s), active virus checking must be performed, preferably on a standalone computer and/or test server, thus having no communication links to other systems.

The following provisions, which apply to the use of all computers, govern all users:

- Only software purchased by Enfield Council and approved by Digital Services may reside on Enfield Council computer equipment including PCs and mobiles
- Digital Services will undertake to purchase licences for all products used by Enfield Council and will control the allocation of licences for products that are distributed as single media items and licences for multiple instances of that one distribution
- Only Digital Services authorised technical staff may install or remove software on Enfield Council computer equipment
- Software includes source code, object code and intermediate code that can be firmware as well as software
- Downloading of 'shareware' and/or 'freeware' is prohibited irrespective of the fact that a licence may or may not be needed unless Digital Services has approved the product to be downloaded and installed
- The installation of personal software including screen savers is prohibited
- Upgrades to software products will be treated as new products
- All software media is to be held and securely stored by Enfield Digital Services
- Digital Services staff may copy software media only if they are legally allowed to do so. This is in accordance with Copyright laws and the terms and conditions of the relevant software license. Software media may not be copied under any other circumstances.

Mobile computing

When using computing and communication facilities outside of the secure office environment, special care should be taken to ensure that information is not compromised. Protection must be in place to avoid unauthorised access to or disclosure of information including ensuring your screen cannot be seen by others and that equipment is not left unattended.

If a device is lost or stolen, the DS Service desk must be contacted as soon as possible.

Access from overseas

Access to the council’s network from overseas is subject to additional controls to ensure compliance with relevant legislation and this may place additional personal liability on users.

Access from countries with a 'decision of adequacy' from the UK Information Commissioner is generally permitted for Enfield Council information assets, but not for those owned by others such as data entrusted to the council by Department of Work and Pension (DWP) – please seek advice from the DS Service Desk before taking devices with access to non-Enfield data overseas.

The user should seek advice from the DS Service Desk before taking any council supplied IT equipment outside the United Kingdom. The equipment may not be covered by the council's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel. Network security systems in place will also flag overseas access and the user will be excluded from the network services as a result. See Smart working Policy on the staff intranet page.

Printing

Users are encouraged to print only when necessary and to use double-sided printing to conserve paper and reduce costs. Please print in black and white, which is set as the default, unless colour printing is absolutely necessary.

Collect printed documents promptly to prevent unauthorised access to sensitive information.

Avoid large print jobs during peak times to prevent printer overload. For very large volumes, please use the council's print department.

Print activity will be regularly monitored to identify trends and areas for improvement.

Fax

All faxes must include a non-disclosure statement and security classification.

All users must ensure that confidential faxes are protected during transmission and only sent when the recipient is aware of the transmission and is instructed to protect its content.

Confidential faxes must be removed as soon as the transmission has ended.

Telephones

Personal calls should be kept to a minimum and not interfere with performance of duties. The council reserves the right to check, review and monitor telephone calls made using any council telephone or telephone system.

Where the council provides a user with a mobile phone, it is to ensure that the user is contactable when away from the office. Therefore, council mobile phones should be switched on or directed to voicemail or an alternative phone at all times during working hours.

Voicemail should be checked regularly and greetings updated as necessary. Voicemail users should secure their messages with a minimum four-digit pin code and clear down messages on a frequent basis.

To ensure that a mobile phone cannot be used fraudulently, it should be protected by using a PIN number. If a council mobile phone is lost or stolen it must be reported to the DS Service Desk.

Legislative requirements

Under no circumstances are users allowed to engage in any activity that is illegal under local, national or international law while utilising council resources.

Whilst using the council smart mobile devices any attempt to change the SIM card or in any way alter the IMEI information of the device is a disciplinary action by the council and a punishable offence under UK law.

Monitoring use

The council reserves the right to monitor, review and record the use of all information and telephone systems and all documents stored on information systems, including documents profiled as private and confidential.

The council may exercise this right in order to establish facts relevant to council business and to:

- comply with regulatory practices and procedures
- prevent or detect crime
- ensure compliance with council policies
- investigate or detect unauthorised uses of the system or to ensure the effective operation of the system (for example, to check if viruses are being transmitted)

Therefore, users do not have the right to complete privacy when using council information systems or in relation to any communications generated, received, processed or stored on council information systems.

Policy compliance

The council expects that all users will comply to the directives presented within this policy. This policy will be included within the Information Security Internal Audit Programme, and regular compliance checks will take place to review the effectiveness of its implementation.

Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question:

- If complying with the policy would lead to physical harm or injury to any person
- If complying with the policy would cause significant damage to the company's reputation or ability to operate
- If an emergency arises

In such cases, the user concerned must take the following action:

- Ensure that their manager is aware of the situation and the action to be taken
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report
- Ensure that the situation is reported to the DS Service Desk (who will inform the DS Security Manager) as soon as possible

Failure to take these steps may result in disciplinary action.

In addition, the DS Security Manager maintains a list of known exceptions and non-conformities to the policy. This list contains:

- known breaches that are in the process of being rectified
- minor breaches that are not considered to be worth rectifying
- any situations to which the policy is not considered applicable

The council will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

Penalties

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorised disclosure or viewing of confidential data or information belonging to the council or partner organisation

- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of the council or partner organisation to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the DS Service Desk or senior management

Any violation or non-compliance with this policy may be treated as serious misconduct.

Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.

View the Acceptable Use Policy declaration (PDF, 124.77 KB).

Policy details

Author – Information Governance Manager
Owner – Information and Data Governance Board
Version – 6.3
Reviewer – Information and Data Governance Board
Classification – Official
Issue status – Final
Date of first issue – 20.08.2009
Date of latest re-issue – 30.05.2024
Date approved by IGB – 19.05.2024
Date of next review – 30.04.2025

Council news directly to you

The latest news in your inbox every week. Council news, community updates, local events and more.

Sign up

Civic Centre
Silver Street
Enfield
EN1 3XA

View Civic Centre on map

- Contact us
- Privacy notice
- Terms of use
- Organisation structure
- Feedback and complaints
- Cookie policy
- Accessibility statement
- Raise a Member's Enquiry

Connect with us

© 2025 Enfield Council