Harlow
Council
Working together for Harlow

Harlow Council

ICT Acceptable Use Policy

Effective date 19 June 2023

Document Information

Policy Author(s):	**Glenn Spreadbury**	Document Version No:	**0.6**
Service	**Governance**	Document Version Date:	**27/05/2023**
Department	**ICT**	Document Type:	**Policy**

Contents

1. ICT Acceptable Use Policy

The purpose of this policy is to provide guidelines for the responsible and acceptable use of information and communication technology (ICT) resources within Harlow Council. The policy outlines what constitutes acceptable use and sets clear expectations for all users of Council systems and hardware when accessing ICT resources. This policy is designed to protect the security and confidentiality of Harlow Council's information, systems and Data Protection as well as to ensure the efficient and ethical use of ICT resources for business purposes. This Policy supports the GDPR Accountability Principle

1.1 Scope

This policy applies to all ICT resources owned or operated by the organisation, including but not limited to computers, laptops, smartphones, software, networks, servers, data storage devices, email, and messaging systems applications.

Acceptable use means that use of equipment and access to information is legitimate in delivering Council services and enacting Council business. Equipment and information is used as authorised, 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 of equipment and information complies with relevant legislation and regulation.

The Council aims 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, IT services and associated assets, however caused, could have potentially devastating consequences for the Council and may result in financial loss and legal action.

1.2 Who does this policy apply to?

All permanent Harlow Council employees, casual employees, contractors/agency staff, Members, consultants, suppliers, and business partners (referred to in this Acceptable Usage Policy "Policy" as "Users") with access to Harlow Council information and information systems and assets.

1.3 Policy statements

It is the responsibility of all Users to know this Policy and to conduct their activities accordingly. By utilising Harlow Council issued equipment or systems, Users agree to comply with this Policy. An appropriate warning notice is displayed to this effect each time when Users log into Council run systems stating "You are about to log in to Harlow Council's network. You should not proceed unless you have approved credentials issued to you by ICT team, and the account you are intending to use is not shared and does not belong to another user. By logging into this system you are agreeing to the IT policies stated on the Council's intranet at the following location: https://www.harlow.gov.uk/kaonet/our-policies-plans-and-strategies. As use of Harlow Council systems you are responsible for ensuring that you read and understand the content of these policies and that you comply fully with them. In accepting this message and proceeding further you are formally accepting that you do understand the policies, accept their content and will comply with them".

Breach of the Policy by any User could result in disciplinary action or other appropriate action being taken.

Council information and IT facilities are provided for Council business purposes only, with limited personal use, during non-working time, permitted as defined elsewhere in this Policy. Users are responsible for exercising good judgment regarding the reasonableness of personal use of ICT resources against compliance with Officer's Code of Conduct.

Users should be aware that any data they create on Council ICT systems (including anything pertaining to themselves) is deemed to be the property of Council. Users are responsible for their own actions and should ensure professionalism and decorum is upheld when communicating (be it in writing or otherwise) with colleagues, suppliers, partners, and members of the public where appropriate.

For security and network maintenance purposes, authorised persons 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. Concerns about misuse of company devices or systems if observed, should be reported to a member of the senior management team as named in the Council's Whistle-Blowing policy, to maintain integrity and accountability within the Council.

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

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

2. User IDs and Passwords

Users must:

2.1 Have a unique User account to access Harlow Council systems and set a password for this. The password must not contain any personal information and must be kept confidential by the User.

2.2 Create strong passwords for each User account that meet the Council's configured rules to maintain the security of their accounts, avoiding common words and personal information such as names and dates. Users are responsible for keeping their passwords confidential and should never share their passwords with anyone.

2.3 Never share User accounts as this is strictly prohibited. Each User is responsible for their account and any actions taken through the account, regardless of who has made changes or access.

2.4 Own responsibility to change their passwords in line with the Council's configured rules to maintain the security of their accounts.

2.5 Contact ICT in the event a password is forgotten. Users are reminded that ICT Service reserve the right to decline any password reset requests which are (in the reasonable opinion of the ICT team) considered suspicious. Authorisation may be required from an appropriate member of the management team.

2.6 Be aware they are solely responsible for the security of their User IDs and passwords. Harlow Council will not be responsible for any unauthorised access to User accounts following the breach of any guidance within this Policy.

3.Managing and Protecting Information

Users must:

3.1 Maintain the confidentiality of all data, and Confidential Information, including but not limited to, strategic, financial and Personal Data stored within the Council's systems.

3.2 Be aware that access to Harlow Council's information systems must be limited to authorised individuals. Any access privileges servicing other IT systems managed by third parties will be periodically reviewed, and access to those systems revoked where appropriate.

3.3 Understand Council information systems and resources may only be used for Council business-related purposes. Personal use of ICT resources is prohibited, except for limited and incidental personal use, during non-working hours. Any personal use must not interfere with the Council's operations or compromise the security of Council information.

3.4 Under the MOU with the DWP you must not use personal devices to access the DWP, HMRC and/or Home Office derived data and/or systems as they are not compatible with these requirements (personal devices include mobile phones and personal laptops).

3.5 Be aware that access to DWP, HMRC and/or Home Office data made available to LAs will only take place from within the United Kingdom (UK) – no solution allowing individuals or CSPs access from outside of the UK will be permitted.

3.6 Ensure that all data is securely saved into an appropriate location on the Council's network and not directly onto any device. Users are responsible for the appropriate and correct storing of Council and Personal Data to mitigate failures of local hardware and loss of Council and Personal Data.

3.7 Only create, store, transmit or otherwise process data made available by DWP by ICT and/or information systems which are located within the UK.

3.8 Take appropriate steps to protect Council systems, hardware and Council and Personal Data from physical damage and environmental hazards, such as fire, flood, or theft.

3.9 Not attempt to access, amend, damage, delete or disseminate another Users files, emails, communications, or data without prior written appropriate authority.

3.10 Acknowledge and comply with any HR guidance or policy in handling employee Personal Data.

3.11 Ensure they are not overheard or overlooked in public areas when conducting Council business.

3.12 Not attempt to compromise or grant or gain unauthorised access to Council ICT systems for any purpose. All or any to access to Council ICT systems is subject to prior written consent via the relevant line manager or AD through the ICT Portal. Each consent must be recorded for audit purposes.

3.13 Not transmit copyright software from any Council ICT hardware or system or allow any other person to access it from any Council ICT hardware or system unless the ICT team have confirmed that the controls or licence permits

3.14 Not 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 prior permission from that other person or organisation

3.15 Not copy/install copyright software from/to any Council ICT hardware or system for any purpose not previously approved by the licence and or for which Harlow Council does not have an active licence

4. Appropriate use of Harlow Council issued equipment.

Users must:

4.1 Understand they are personally accountable for their actions when online whilst utilising Council systems or devices.

4.2 Understand the Council allows use of personally owned ICT equipment for personal use and on a private network, limited to non-working time.

4.3 Understand use of these resources must not be used for illegal or unethical purposes, including, by way of example and not limited to:

- Spamming or sending unsolicited emails.
- Distributing viruses or malicious software.
- Hacking or attempting to access unauthorised resources.
- Infringing on intellectual property rights.
- Engaging in any activity that is damaging to the Councils ICT equipment resources or network.
- Access to, or promotion of, activities related to illegal activities, including terrorism related content

4.4 Understand that storing their own data, including photos, on Council equipment is prohibited.

4.5 Ensure any activity performed on a Harlow Council ICT asset does not damage the reputation of Harlow Council, its Elected Members and those living in its District which includes accessing or distributing links or content that:

- Could cause embarrassment or compromise Harlow Council in any way.
- Breaches any copyright or licensing agreement.
- Could be interpreted as harassment or insulting to others.
- Is in anyway offensive, indecent or contains obscenities in text or images.

4.6 Understand the following when utilising Harlow Council ICT systems and internet connectivity, whilst acting in the capacity of your professional role for the Council

4.7 You must not:

- carry out personal or business transactions that are not related to your work; including accessing of banking or shopping sites.
- Publish or share any views, beliefs or commitments which could be interpreted as the views of the Council.
- Use any behaviour that is discriminatory in any sense
- Act in a way that undermines or damages implemented management or security controls.
- Incite hate, bullying and harassment.

- Access any on line site or resource containing but not limited to the following categories: - pornographic, gaming, gambling, drugs or hate.
- Download or install software onto Council issued ICT equipment, except for relevant mobile applications in line with corporate usage. (E.g.: Office 365 applications/Authenticator/Committee papers etc)
- Access any personal email account on Harlow Council ICT equipment unless, after seeking approval from the relevant line manager or AD through the ICT Portal the access is deemed relevant for Council business purposes.
- Download music, video or other media-related files for non-business purposes which may breach licensing or copyright, or store on Harlow Council equipment.

4.8 Harlow Council will not accept any liability for any loss, damage or inconvenience that may be suffered from the improper or personal use of its ICT systems or equipment.

5. Email, Voice, Messaging, and conferencing systems.

Users Must:

5.1 Comply with the Council's Electronic Communications Policy

5.2 Use appropriate and professional language in messages, emails, recordings, and all conferencing facilities and behaviour in line with the Officer's Code of Conduct.

5.3 Never engage in the transmission of any types of unsolicited Email.

5.4 Never alter the body or contents of a third party email communication when forwarding unless authorised or requested to do so by the that third party.

5.5 Be vigilant to spoofed or scam email or messages especially when they are specifically targeted to imitate legitimate email or correspondence.

5.6 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 may be fake - the Council and its third parties will never ask for these details.

5.7 Never attempt to assume or assume the identity of another User or create any or send any material in the attempt to mislead anybody in masking the origin of the email or message.

5.8 Only use or add digital or scanned signatures with appropriate recorded prior permission. (In a test setting or environment with appropriate permission assuming identity or an account or resource is acceptable if the relevant permission is sought.)

6. Websites and social media

Users must:

6.1 Treat access to social media accounts as view only where utilisation to post for business purposes has not been granted; access to social media platforms (to view Council communication and resident response) is provided for all Users for Council business purposes only.

6.2 Only utilise approved social media accounts for Harlow Council business or communication if the appropriate permission has been obtained and the use of official branding and standards are met. Users are fully responsible for the content they post online within any platform or forum, and any posts must meet the requirements of the platform or forum.

6.3 Understand that all social media content/footprint may be available for anyone to view, indexed by external sources and archived for posterity.

6.4 Only access content appropriate to business functions, and not intentionally visit or utilise any site or resource which may contain explicit, indecent or advocate any illegal activity. The blocked category list (managed by ICT) includes content related to indecent and inappropriate material, e.g. sites containing malicious links, sites related to illegal activities (e.g. terrorism related material), asites related to gambling or pornographic material. Access to blocked sites can be made available on request with details of legitimate business reason for access, and access granted to any blocked category listed sites must be recorded through the ICT portal and viewed from a connection segregated from any Council owned circuit or device.

6.5 Raise a relevant request using the ICT Portal, for access to sites which are blocked no matter the category or content. By no means should a User attempt to bypass security measures or utilise another device managed by Harlow Council to view blocked material.

6.6 Alert the ICT Service through the ICT Portal if you have accessed a service or site (or witnessed the accessing of a service or site) which would be deemed inappropriate or fall within the non-permitted list as specified in this or any other policy relevant to internet usage.

7. Devices, Systems and Network access

Users must:

7.1 Only utilise systems, applications, software, appliances, and devices, (including removable storage, laptops, and smart devices), which are approved, procured, configured, and managed by Harlow Council ICT service when undertaking business activities.

7.2 Understand the responsibility when utilising equipment externally, (Including Workstations, Mobiles, Tablet and Laptops)

7.3 Equipment used for Council business activities remotely such as home equipment requires updating by the end User when appropriate or prompted. Failure to complete updates to external equipment may result in the termination of the connection into Council systems.

7.4 Be aware where two factor authentication is present, Users can obtain permission through the ICT Portal for Microsoft 365 applications to be installed to a compatible/secure personal device in the absence of a Harlow Council managed device. (Requests for a Council device can be made through the ICT Portal). Harlow Council will not reimburse any User who has requested the installation of sandboxed corporate applications onto a Users personal owned device.

7.5 Ensure no sensitive or restricted or Personal Data is stored on portable devices and must utilise appropriate shared folder locations when handling Council documentation.

7.6 Not use personal wallpapers or screensavers. Corporate photos should be used for profiles on all platforms. The use of personal suitable backgrounds on Microsoft 365 meetings is acceptable but must be respectful and not contain any inappropriate or offensive imagery that may bring the User or Council into professional disrepute.

7.7 Not use personal devices for training purposes. Adequate training facilities are available on request through the ICT Portal . External equipment from providers or partners should not be plugged into any internal network point. Appropriate connectivity to a segregated internet connection can be provided, if necessary, on request through the ICT Portal . It is the responsibility of the User booking training facilities to ensure all external parties have the appropriate resource in place with adequate notice.

7.8 Raise all software requests using the ICT Portal or through the relevant application owner if not provided by ICT.

7.9 Not use Council issued mobile devices abroad. This is forbidden unless authorised at Director level, connectivity must be in line with the guidance within this policy. Access from countries with a 'decision of adequacy' from the UK Information Commissioner is generally permitted for Harlow 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 ICT Service Desk before taking devices with access to non-Harlow data overseas.

7.10 The User should seek advice from the ICT 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

The Council will:

7.11 Carry out a remote wipe of data in the event of loss or disciplinary proceedings where a personal device is approved and utilised for Council business., Harlow Council will not be liable in loss of Personal Data if a remote wipe to a personal device to remove corporate data affects the operability of the device or its contents.

7.12 Permit the use of personal peripherals such as (Headsets, keyboard, mice) to be connected via cable or Bluetooth to Harlow Council equipment. No personal devices containing storage that can be transferred are to be connected to Council equipment including, but not limited to:

- Phones
- Cameras
- Tablets
- Portable storage devices

7.13 Permit the use of personal mobile devices and landlines for voice calls in unavoidable circumstances only, which include internal and external calls to staff within the Council or other government departments, local authorities, and business partners, however personal or sensitive information should not be discussed. Where access is available to a Council managed softphone or mobile device this is the preferred method of communication.

7.14 Permit 4/5G connectivity and home broadband connectivity to connect back into Harlow Council systems through the appropriate corporate solution via Wi-Fi or ethernet. However, the use of internet connections that use landing pages for agreement to use or using VPN solutions to change the origin of the connection, are strictly prohibited when connecting into Council systems. ICT cannot support personal home internet connections for remote working which are proven to be intermittent or lack the bandwidth required for stable connectivity.

8. Physical Security

Users Must:

8.1 Be responsible for the safety and security of all portable devices assigned to them. Users are responsible for the immediate report of any loss, damage or theft and raise the appropriate incident request with Police where applicable.

8.2 Protect Harlow Council issued equipment appropriately when travelling, including but not limited to:

- Never leaving devices within parked vehicles
- Never leaving devices unattended when off site or in a non-secure setting
- Laptops must only be carried as hand luggage when travelling abroad or internally, where permission has been correctly sought.

8.3 Be responsible for the return of all equipment when leaving Harlow Council, including physical return to the Civic Centre under safe carriage, including details of PINs used and any costs associated with this. Failure to return equipment could lead to steps being taken to recover any loss incurred by the Council, which may include legal action.

9. Compliance

9.1 If any User is unable to comply with this Policy or requires use of assistive technology which is outside of the scope of this document, this needs to be documented and raised with a line manager and Human Resources for advice and assistance.

9.2 All requests to use currently unapproved software must be subject to investigation by the ICT Service and subject to an approval process.

9.3 Line managers are responsible for ensuring that Users understand their responsibilities as defined in this Policy and continue to meet its requirements for the duration of their Harlow Council employment. They are also responsible for monitoring employees' usage of Harlow Council systems. This does not remove responsibility from employees, who must ensure that they too understand their responsibilities as outlined in this Policy and continue to meet the requirements.

9.4 Any violation or non-compliance with this Policy may be treated as serious misconduct. Penalties may include termination of employment or contractual arrangements, or prosecution.

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

9.6 The Council reserves the right to monitor email traffic within the corporate email system and to access mailboxes and private directories without notification to the individual concerned that the right is being exercised.

9.7 As an employer the Council has the right to monitor communications within the workplace and uses a statement upon log-in to the Council's environment to ensure users are aware of the monitoring as laid out below before accessing Council systems (as also included in previous iterations of Conditions of Acceptable usage Personal Commitment Statement which this policy replaces) . Monitoring can cover:

- emails
- internet access
- telephone calls
- data

- images

9.8 The Council may exercise this right in order to establish facts relevant to Council business and to comply with:

- Regulatory practices and procedures
- Creation of responses to FOI or SAR submissions
- To prevent or detect crime
- To ensure compliance with Council policies, including this policy and the Officers Code of Conduct
- To 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)

9.9 Therefore, Users do not have the right to privacy when using Council information systems or in relation to any communications generated, received or stored on Council information systems.

10. Information System Security

Users Must:

10.1 Process Personal Data only in accordance published privacy notices or current informed Consent.

10.2 Act in accordance with data protection principles and Council information governance policy, including information retention periods

10.3 Lock their workstation or close it down when unattended

10.4 Not leave paper copies of data, memory sticks or other portable media on desks when unattended.

10.5 Ensure that GDPR training is undertaken

Contact Information:

For any questions or concerns regarding any policy contained within this Policy, please contact the ICT Service on 01279 446789.

Version History

Date of this revision:	May 2023
Date of next planned revision:	May 2025

This policy replaces the previous Conditions of Acceptable usage Personal Commitment Statement

Version No:	Version date	Summary of Changes	Revised by
0.1	Feb 2023	First draft	G. Spreadbury
0.2	Mar 2023	Second Draft	G. Spreadbury
0.3	April 2023	DPA review	J. Galvin
0.4	May 2023	Fourth draft	G. Spreadbury
0.5	May 2023	WLT review	WLT
0.6	May 2023	HR and Trade Union review	N. Terrell