IT acceptable use policy

Author: Donna McLeod

Contact: Donna.McLeod@luton.gov.uk

Version: 5.3 (published)

Last updated: January 2026

Document History

Version	Date	Notes	Prepared by
1.0	01/08/2022	Created	Leigh Jolly
3.1	31/10/2023	Reviewed	Hazel Lunn
5.0	28/09/2024	Revised – updated with AI, MS teams, working from abroad	Donna McLeod
5.3	12/02/2025	Revised MS Team Guidance	Donna McLeod

Contents

1. Purpose, scope and responsibilities

1.1 Purpose

1.1.1 To ensure that access to council, trust and customers data is protected by measures that are appropriate to the sensitivity of the data or systems and that access control measures comply or exceed the minimum necessary standards imposed by legal statute other mandatory requirements.

1.1.2 The Acceptable Use policy (AUP) aims to protect all users of Luton Council IT equipment and data and minimise risk by providing clarity on the behaviours required by Luton Council IT users.

1.1.3 To ensure that individuals understand their responsibilities for the appropriate use of Luton Council's information technology resources.

1.1.4 To ensure that users are aware that any data they create on council systems is deemed property of the council.

1.2 Scope

1.2.1 This document applies to all Councillors, Committees, Departments, Partners, employees and workers of the council, employees of local trusts who use council IT whilst providing services on behalf of Luton Council, contractual third parties and agents of the council and trusts who use Luton Council provided IT facilities and equipment, or have access to, or custody of, council or trust customer information. These people will be referred to as 'users' in this document.

1.2.2 All Luton Council equipment and information (all information systems, hardware, software and channels of communication, including voice-telephony, social media, video, email, instant messaging, internet, generative AI and Large language models, and intranet). User's personal information which is processed by council equipment is also subject to this policy.

1.3 Responsibilities

1.3.1 All users must understand and adopt use of this policy and have a responsibility for ensuring the safety and security of the council's infrastructure, hardware and software and the information that they use or handle. Failure to comply with the policy may be a disciplinary matter.

1.3.2 All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds and must report incidents and breaches timely to minimise risk.

1.3.3 When a request to review emails from the council vault is made it must be authorised by the Service Director, Customer and Organisational Development, or Monitoring Officer, or their representatives. This also applies if legitimate access to an absent person's system or data is required.

1.3.4 Council equipment must be provided for inspection on request. Users must not remove or deface any asset registration numbers.

1.3.5 When a user leaves the authority, all items must be returned to the technology team on the employees last day. Password & codes for mobile devices must also be provided. Failure to do so will result in a charge for replacement equipment.

1.4 Supporting Documentation

You are advised to read the following supporting documents.

- Social Media policy
- Data Protection policy
- Artificial Intelligence policy

2. Acceptable use principles

General principles

Do

- Read and agree the acceptable use policy in its entirety.
- Immediately report and breaches
- Understand that the council's systems are monitored and audited frequently.
- Complete the Cyber Awareness Training
- Complete the GDPR Training

Do not

- Undertake illegal activity

2.1 Users must:

2.1.1 Confirm prior to use of Luton Council equipment or information that they agree to comply with this Acceptable Use policy

2.1.2 Be responsible for their own activity and act responsibly and professionally, following the councils code of conduct and respecting colleagues, suppliers, partners and customers.

2.1.3 Immediately report any known or applicable breach of this policy to their line manager and comply with official procedures when a breach of the policy is suspected or reported.

2.1.4 Never undertake illegal activity, or any activity that would be harmful to the council's reputation or jeopardise staff and/or customers data by use of councils IT.

2.1.5 Understand that both business and personal use of Luton Council systems and communication channels will be monitored to maintain effective operation and comply with audit requirements or financial control. (See 7.2). Any relevant information may be produced in any investigation or hearing relating to an alleged breach of council standards, policies or procedures.

2.1.6 Undertake annual data protection and quarterly cyber security awareness training. Specific roles may also require regular updates in organisational policies and procedures and specific training as they may be more vulnerable to attack.

3. Managing and protecting information

Do

- Ensure that data is recorded accurately, shared and disposed as per the retention schedule
- Verify the person you are communicating with
- Be aware of your surroundings
- Lock your device when you leave your workstation (Windows Key + L)
- Keep your password confidential

Do not

- Attempt to access anyone's personal data without a business need – this includes information relating to you personally
- Provide information to those whose identity cannot be verified
- Attempt to bypass security access controls put in place
- Share your passwords

3.1 User must

3.1.1 Understand that they, and the council, have a legal responsibility to protect personal and sensitive information and must not misuse their official position to further private interests or those of others.

3.1.2 Ensure that all information is created, used, shared and disposed of in line with business need and in compliance with all data relevant policies listed in the relevant policies section of this document.

3.1.3 Not attempt to access anyone's personal data unless there is a legitimate business need that is appropriate to their job role.

3.1.4 Users must not, knowingly access, or attempt to access, their own council records or the records of family members or anyone else known to them – this includes information held within information assets and paper files.

3.1.5 Not provide information in response to any type of request whose identity they cannot verify.

3.1.6 Be aware of surroundings and try and make sure they are not overheard or overlooked in public areas when conducting council business. This includes use of laptops and mobile phones. See Data Protection policy for more information.

3.1.7 Not attempt to compromise or gain unauthorised access to council information

3.1.8 Users must lock their workstation, if they are leaving unattended – this includes if working in remote locations, including home.

3.1.9 Respect the controls in place to protect the network, by-passing or downloading unapproved programmes is prohibited, on any end user device (smartphones / laptops)

3.1.10 Keep passwords confidential, if you are suspicious that this has been compromised, change it.

4. Personal use of Luton Council IT Resources

Do

- Understand you are accountable for online activity
- Understand personal use is permitted within your own time
- Limit the storage of personal data to the hard drive
- Understand that any data stored can be accessed by IT staff
- Understand the council is not liable for any negative consequence as a result of personal use
- Behave responsibly and be aware of the council's standards of behaviour (4.6 & 4.7 below)
- Be aware that the default setting on the calendar is Open to all to view title and location – use privacy where applicable

Do not

- Use a data sim for personal use
- Access personal webmail accounts from a council device

4.1 Users must:

4.1.1 Understand that they are personally accountable for what they do online for work and personal use with Luton Council technology.

4.1.2 Understand that the council allows personal use of its IT resources within the limit of this policy, in an employee's own time, and that the device is connected to wifi, not through a data sim

4.1.3 Limit the storage of personal information to local hard drives, and where it is stored ensure that any of their data stored is appropriate i.e., legal, applicable, and compliant with this policy and GDPR legal requirements.

4.1.4 Understand that the ability to store personal information on the local hard drive of council owned devices and systems is a privilege and the council has a right to require the data is removed should this data interfere with business activity or use.

4.1.5 Ensure personal activities do not damage the reputation of Luton Council, its employees and customers including accessing, storing, transmitting, or distributing links to material that:

- Could embarrass or compromise the council in any way.
- Is obtained in violation of copyright or used in breach of a licence agreement.
- Can be reasonably considered as harassment of, or insulting to, others.
- Is offensive, indecent, or obscene including abusive images, language, and literature.

4.1.6 Understand that the council does not accept any liability for any loss, damage or inconvenience you may suffer because of personal use of its IT.

4.1.7 Follow the Luton Council's standards of behaviour and **must not**:

- Send messages or material that solicit or promote inappropriate religious, political or other non-business-related causes, unless authorised by the council
- Provide unauthorised views or commitments that could appear to be on behalf of the council.
- Use malicious, harassing, abusive or threatening communication.
- Incite hate, bullying and harassment.
- Visit pornographic sites or undertake any form of gaming, lottery or betting.
- Use unlawful behaviour that is discriminatory in any sense (ie on the grounds of age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion/belief, sex or sexual orientation)
- Use any means to circumvent management or security controls or damage, destroy, or deny availability of service.
- Access personal webmail accounts on council equipment
- Download music, video or other media-related files for non-business purposes or store such files on network drives

5. Email and Calendar Use

Do

- Use egress to send emails that are going external and contain personal identifiable, sensitive or financial information.
- Report any suspicious emails/activity by calling 01582 546666
- Advise participants if a conference call is being recorded
- Check content is suitable if using a “reply all”
- Ensure your emails have a relevant subject line
- Include an email signature to help the recipient understand who the email is from
- Use BCC when emailing a number of people who may not known to each other
- Maintain good email hygiene by regularly reviewing cached email addresses
- Regularly archive your calendar – the recommended time is 90 days
- Ensure you mark any PII data within your outlook calendar as a private appointment – this applies to customer and personal information

Do not

- Auto forward emails to a personal email address
- Alter emails when forwarding, unless specifically instructed
- Misuse scanned signatures
- Use an LBC email address for personal use
- Forward payment card information on any channel
- Contact international or premium numbers without permission
- Use a personal mobile phone or email address to contact service users

5.1 Users must:

5.1.1 Not knowingly engage in mass transmission of unsolicited emails (SPAM).

5.1.2 Protect emails using egress, when emailing information that includes personally identifiable information, or financial, sensitive or other information that could cause detriment to the council or an individual

5.1.3 Never auto forward email to external accounts

5.1.4 Not alter the content of a third party’s message when forwarding it unless authorised to do so.

5.1.5 Not try to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned signatures).

5.1.6 Be vigilant to scam targeting communications especially phishing emails and know how to spot and report suspicious emails. For the avoidance of doubt suspected phishing must always be reported immediately to the IT helpdesk (calling 01582546666).

5.1.7 Not use their council email address for any purpose other than council business or related organisational activity. All employees must use their personal email address for personal activities including purchasing and selling of goods, internet banking, personal social media and any other personal activity.

5.1.8 Be vigilant to ensure that the email is being sent to the intended recipient

5.1.9 Understand that Customer payment card information is stored in specialist systems. Card information is protected and must never be sent via messaging channels, such as Teams and email, or saved outside of the prescribed systems, on the council’s network.

5.1.10 Understand that calling international or premium telephone numbers using council resources is prohibited, other than for legitimate council business.

5.1.11 Not use personal phones to contact service users who should not have access to your personal contact number. This includes all personal mobile phone functionality including SMS texting, instant messaging, social media apps or personal email.

6. Websites and Social Media

Do

- Read the social media policy
- Report websites that should potentially be blocked
- Understand that all activity is tracked and can be reviewed

Do not

- Access inappropriate websites

6.1 Users must:

6.1.1 Comply with the Social Media policy and be aware of council guidelines.

6.1.2 Only access appropriate content using Luton technology and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity, as described in the council's standards of behaviour, (4.7)

6.1.3 Contact the IT Helpdesk with requests to unblock a website and not attempt to bypass the council's web filters.

6.1.4 Report any access to a site that they feel should be blocked by the council's web filters to their line manager and contact the IT Helpdesk with a request to block a website.

6.1.5 Understand that all web traffic is logged for auditing purposes and that logs containing your use of council resources may be reviewed at any time.

7. Devices, systems and networks

Do

- Immediately report lost / stolen devices to the IT Service desk (01582 546666)
- Immediately report any unusual activity
- Use the device frequently, at least monthly to avoid restrictions
- Install updates timely – laptop and mobile
- Return hardware to the line manager on your last day of working, advise if this is not possible

Do not

- Bypass / request work arounds for the security controls in place
- Connect non-LBC devices to the network via cable, unencrypted USB and Bluetooth
- Tether from mobile phones for lengthy periods

7.1 Users must:

7.1.1 Report any security concerns or lost/stolen equipment by telephone to the IT Helpdesk immediately, regardless of their present location.

7.1.2 Understand that equipment is issued with various technical controls. This includes usage monitoring tools for web browsing and mobile data usage. Restrictions are in place on administration permissions to prevent the unauthorised download and installation of software. Certain areas of the council will use call recording solutions for training and monitoring purposes. In these areas it is the manager's responsibility to ensure employees receive adequate training and to ensure that each employee has access to call recording guidelines. Users must not attempt to bypass or circumvent technical controls, or configuration. If there are restrictions on your device that are impeding your work, please contact the IT helpdesk.

7.1.3 Ensure that equipment is returned when it is no longer required or will not be required for a period of three months or more. For the avoidance of doubt, equipment should be returned for staff who are unable to log on every 30 days. Devices must be connected at least once a month in order to continue receiving security updates. A device will be blocked from accessing the network if it has not been used for more than 30 days.

7.1.4 Understand that line managers are responsible for reclaiming equipment at the end of their line report's employment. Difficulties in complying with this requirement must be flagged with the technology team.

7.1.5 Always install the most up to date software as soon as it becomes available on Luton Council mobile phones. This ensures the device has the latest security updates installed. Failure to do so may result in the device becoming restricted from accessing any council systems prior to potential withdrawal of the service.

7.1.6 Not connect any non-corporate devices to Luton Council laptops or any other device connected to the council's infrastructure, for the purpose of uploading/ downloading files, this includes the use of bluetooth technology and charging cables.

7.1.7 Not bypass controls to prevent connection via captive portals, for example a shop or restaurant public wifi that collects your details in order to gain access. The council permits connecting corporate devices, laptops etc by Wi-Fi (or Ethernet) to the internet to connect back to the council from anywhere e.g. home or a hotel. For security reasons council devices are configured so they do not connect to captive portals.

7.1.8 Understand that whilst the council permits wirelessly connecting a corporate device to a mobile phone via a personal hotspot for the purpose of acquiring an internet connection (tethering) it should not be for prolonged or regular use. Tethering a personal mobile phone is also permissible but the council cannot be held liable for any charges associated with using personal devices in the way, and so any use of a personal phone for this purpose is the individual's choice.

7.1.9 Ensure that council information is not knowingly stored on devices without security controls. For the avoidance of doubt, users should assume that devices issued by the council do have appropriate security controls.

8. Access from Overseas

Do

- Seek permission to take equipment overseas
- Check the permitted countries prior to requesting to take equipment overseas

Do not

- Connect to public wifi whilst overseas

8.1 Users must:

8.1.1 Seek permission from their line manager prior to taking council owned assets overseas.

8.1.2 Seek advice from the IT Service Desk before taking any council supplied IT equipment outside of the United Kingdom

8.1.3 Provide a cost centre for any additional roaming services

8.1.4 Not request or take a device if the county visited is not listed under the participating states. The participating states can be found here, under participating countries.

8.1.5 Understand that corporate devices are encrypted, and must not create, enhance, share, sell or otherwise distribute the encryption software during his/her stay in the relevant permitted country.

8.1.6 Not connect to public wifi – the use of home or hotel broadband is acceptable.

9. Generative AI and Large Language Models (LLM)

This includes, but not is exhaustive of ChatGPT, Copilot, OpenAI, Canva

Do

- Maintain human oversight and responsibility for making final decisions on the output produced
- Notify your manager and disclose that Generative AI/LLM's have been used
- Comply with relevant laws and regulations
- Use publicly available data
- When using assistive functionality, such as a minute taker, advise the attendees that this is the case
- Remember that what is uploaded is visible, either by Data Digital and Technology team or by the provider of the LLM
- Note, this is an evolving area, regular updates will be communicated via e-brief and the intranet
- Only use information that you would be comfortable putting in the public domain, unless you are part of a pilot project, and have a Data Privacy Impact Assessment to support your activity
- Use for professional purposes to compliment your output

Do not

- Input personal, sensitive, commercial or financial information into an unsupported application – this includes ChatGPT and Open AI
- Use to store or release non-public records
- Use for private individual records
- Use if you are in doubt about the security or information being input
- Assume that all of the output is factually correct
- Use if data sovereignty practices of the Gen AI LLM supplier contravene and regulatory requirements

9.1 Users must:

9.1.1 Have read and understood the Artificial Intelligence policy

9.1.2 Have completed the annual GDPR training and the quarterly cyber awareness training prior to use

9.1.3 Log a call with the IT service desk to enable features, outlining their understanding and their business case

9.1.4 Provide a cost centre for any paid versions, such as Copilot

9.1.5 Not upload requests that solicit or promote inappropriate religious, political or other non-business-related causes, unless authorised by the council or provide unauthorised views or commitments that could appear to be on behalf of the council.

9.1.6 Not use malicious, harassing, abusive or threatening communication

9.1.7 Not incite hate, bullying or harassment

9.1.8 Not request information on any form of pornography, gaming, lottery or betting

9.1.9 Not use for unlawful behaviour that is discriminatory in any sense, for example on the grounds of age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or religious beliefs, sex or sexual orientation

9.1.10 Not upload files which contain personal, sensitive, financial or commercial information

10. MS Teams Meeting

Do

- Inform all attendees that the meeting is being recorded prior to it starting and when recording has stopped
- Ensure that the recording retention period is adhered to
- Use Teams for chats to informal contacts – these are automatically delere after 30 days
- Use channels to collaborate responsibly
- Always check who any unfamiliar attendees are
- Always have your camera on during meetings, unless otherwise agreed as part of reasonable adjustments

Do not

- Use for meetings with members of the public, or for a formal HR process
- Allow uninvited guests or third party minute taker into the meeting – always check participants are invited
- Use for meetings containing sensitive data, for example – safeguarding

10.1 Users must:

10.1.1 Request access to the record functionality via the information governance team

10.1.2 Understand that recordings are automatically deleted after a period of 30 days – any additional requirements will be managed through the IT service desk as a request

10.1.3 Understand that data stored within the teams chat and recordings is subject to the Freedom of Information and Subject Access Requests.

10.1.4 Have completed their annual GDPR training

10.1.5 Report any data breaches to the information governance team