

IT Policy e-Safety and Usage Guidance

Luton Adult Learning

Author: Senior Management Team

Contact: info@ltonacl.ac.uk

Version: 1.0 (published)

Last updated: April 2024 (new email address for data breaches)

Contents

Luton Adult Learning	1
Our Aim.....	2
Confidentiality, Information Sharing and GDPR.....	2
E-Safety risks.....	2
Content	2
Contact	2
Commerce	3
Security	3
Education and Training	3
Incidents and Response	3
Expectations	4
Support in place for learners	4
LAL Netiquette Guide for Online and Blended Learning Courses	5
Guidance for staff on working from home	6
General Guidance for Staff and Learners	7

Luton Adult Learning (LAL) is a direct delivery service within Luton Council

Our Aim

Luton Adult Learning aims to ensure that:

- our learners are able to access all of the resources they need online to complete their courses successfully
- our staff have the equipment and resources to deliver online and blended learning courses effectively from Arndale House or from home
- our staff and learners are provided with sufficient support and guidance to enable them to work safely online

Confidentiality, Information Sharing and GDPR

LAL will ensure that it can demonstrate full compliance with the principles of the General Data Protection Regulation (GDPR). All staff are required to complete Luton Borough Council data protection/GDPR training annually and to be familiar with Data Protection legislation. If an employee suspects a data breach has occurred they should report this to their line manager immediately. A data breach report should be completed and sent to dataprotection@luton.gov.uk as quickly as possible and as a maximum within 24 hours. More information can be found on the staff intranet: <https://lutonbc.sharepoint.com/sites/business-intelligence/SitePages/Data-breaches.aspx>

E-Safety risks

E-safety risks can be summarised under the following three headings:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance, sites promoting radicalisation or pornography
- Exposure to illegal material, such as images of child abuse
- Illegal downloading of copyrighted materials e.g. music and films

Contact

- Grooming using communication technologies, potentially leading to sexual assault, child sexual exploitation and radicalisation
- The use of assumed identities on gaming platforms
- Bullying via websites, mobile phones or other forms of communication device
- Spyware, e.g. use of Remote Access Trojans/Tools to access private information or spy on their victim.

Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Security

Luton Borough Council will do all that it can to make sure the Adult Learning network is safe and secure. Security software will be kept up to date. Appropriate security measures will include the use of enhanced filtering and the use of appropriate firewalls, servers and routers, to prevent accidental or malicious access of Luton Borough Council systems and information.

Luton Borough Council complies with guidelines set out by the Counter Terrorism Internet Referral Unit (CTIRU) and has a statutory duty to ensure their systems cannot be used to access any of the websites on the CTIRU list.

Education and Training

With the current unlimited nature of internet access, it is impossible for Luton Adult Learning to eliminate all risks for learners. It is our view therefore, that Luton Adult Learning should support learners to stay e-safe through regular updates and information sharing. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Staff will take part in mandatory Safeguarding training (which includes e-safety) with updates annually. This will be monitored by the Designated Safeguarding Officer. There will also be regular full Service updates. New online threats that are discovered will be shared so that staff can share these with learners, keeping them as up-to-date as possible.

Incidents and Response

When an e-safety incident is reported it will be dealt with very seriously. The management team will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to any member of staff, this will then be passed on to a member of the management team or a safeguarding champion as appropriate. Following any incident, Luton Adult Learning will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Expectations

The expectations of teaching, learning and assessment within LAL apply to all face to face, blended and remote learning. These include but are not limited to:

- learning materials being of a high standard, relating to the intended course learning outcomes and being inclusive, current and accessible to distance learners
- complex ideas being presented in more than one format and/or using an approach to support different learning styles
- activities to consolidate learning and contribute to learners' wider skills development, with further relevant reading and development opportunities being signposted
- learner work being assessed by teachers and assessors including detailed feedback being provided
- learners being guided by teachers and assessors to the right learning resources to improve their work
- learners' personal details not being stored by staff on a personal home computer, but instead being kept in a secure location on the central R drive
- where a session is recorded, all learners knowing and agreeing to its being recorded and where it will be stored for what purpose and timeframe
- teachers ensuring they have suitable evidence for RARPA/ accreditation and audit purposes
- learning materials, including pictures and videos, complying with copyright restrictions
- LAL learners being signposted to the online End of Course Evaluation form for completion
- remote learning being accessible, including adherence to accessibility guidance relating to web-based materials
- staff being supported through workforce development opportunities to develop the skills they need to deliver remote learning effectively and safely

Support in place for learners

All learners at Luton Adult Learning (LAL) will have support that will enable them to complete their learning journey effectively.

Our support includes:

- free Wi-Fi available for all learners on our main campus subject to accepting our Acceptable Use Statement. Select [LBC-Guest-Arndale](#) network. The password is available to you once you are in the building.
- a policy that encourages you to bring your own devices in to the centre if you have them, including laptops, tablets and mobile phones
- laptops being available for use within the centre to provide you with online access within your class times
- laptops being available for use in our learner hub area to provide you with online access during centre opening times: Mon–Wed 9am–5pm; Thurs- 9am-9pm; Fri 9am-4.30pm

- limited availability to decommissioned laptops being possible in cases of hardship. Further information is available from your teacher or please contact info@lutonacl.ac.uk.
- some courses using an on-line Learning Plan to help you to structure your learning and to give you access to all of the resources and materials you need. Some of our courses also use a virtual learning environment (SVLE).
- an online Learner Guide so that you can easily find all of the information you need whilst you are studying here.
- free digital skills training through our service, please ask your teacher for more details.

At this time, the service recommends the use of two video conferencing platforms.

- Zoom
- Microsoft Teams

Though these offer similar features, Zoom is a lot easier to use and is therefore suggested for classroom use. MS Teams offers more business-based features.

LAL Netiquette Guide for Online and Blended Learning Courses

It is important to recognise that the online classroom is in fact a classroom and certain behaviours are expected when you communicate with those engaging with you. These guidelines are known as 'netiquette'.

General Guidelines

- Be on time. Sessions will start and finish according to the timetable. If you join late, please don't interrupt the session. Remain silent and your teacher will support you.
- Be prepared. Come to the meeting with a positive attitude and with any course materials or resources that you have been asked to have ready.
- Where possible, choose a quiet location – away from pets, children, etc. Turn off the TV and any music.
- Be ready to take part. Not everybody is confident in speaking up within a group, especially when you don't already know other learners. However, to make the most of your learning experience we ask that you share ideas, ask questions, and contribute to the discussions.

Security

- Remember that your password is the only thing protecting you from pranks or more serious harm.
- Don't share your password with anyone.
- Change your password if you think someone else might know it.
- Only share an email address or other personal information if necessary.
- If using a webcam, think about what is behind you in view – is it something you don't want others to see?

When communicating online you should always:

- be respectful of others and their opinions
- be careful with personal information (both yours and others')
- beware of using reply all – does everyone need to see your message?
- remember to stay on topic, ask yourself 'Is this relevant to your subject?'

- remember to listen and not talk over each other – this comes with practice!
- mute yourself when not talking
- think about what you are writing or saying, please do not write or say anything that you wouldn't say to someone's face

Please remember we still need to keep each other safe. If you are concerned about your own or another person's safety, please tell your teacher or report it using the safeguarding contact details.

Safeguarding Arrangements

If you have safeguarding concerns that relate to the use of IT please report to our designated safeguarding leads:

- Merielle James - Designated Safeguarding Lead
- Catherine Kirby- Deputy Designated Safeguarding Lead
- Annette Barnby - Deputy Designated Safeguarding Lead

They can be contacted using email, safeguarding@lutonacl.ac.uk

Guidance for staff on working from home

- Be vigilant – no one in your household should have access to or see the personal data you are using.
 - Be aware of your surroundings and who may be able to view your screen/work.
 - Do not write down your passwords on paper where they can be discovered.
- Use strong passwords to protect your work devices and make sure you use a password that no-one else in the household knows or can guess.
- Remember your data protection training to help you to ensure that everything is kept safe whilst at home. Protecting student and staff data must remain the highest priority.
- Data breaches can cause real and significant harm to individuals and the risk of data breaches become much higher when data is accessed remotely or on a portable device.
- Ensure that you use devices provided by the council rather than your own device to access the LAL's network.
- Own devices should only be used with agreement from the IT team. This will help prevent unknown risks to the council's network (such as malware, ransomware or security breaches). In addition to this:
 - check that your device is fully up to date with anti-virus, firewall, malware and security updates
 - ensure that work documents are saved on the R Drive securely rather than on the desktop or in "my documents"
 - ensure your device has a password or (for tablets/phones) pin code and that passwords are complex (a mixture of numbers, letters and capitals)
- Be vigilant to lock screens when not in use for long periods or where you are stepping away from your device. In addition, devices should be shut down at the end of the day.
- Ensure that LAL IT equipment is kept in a secure place. It is your responsibility to ensure that LAL equipment is kept secure (for example in a locked draw). If a device becomes lost or stolen, please report this to Civica, your line manager and the Senior Management Team without delay and within 72 hours.

- Do not install or download any software onto a work device without the approval of the council. Where approval is given, they should also be virus checked before they are downloaded onto the council's systems.
- Always be careful which websites you visit and which emails attachments you open.
 - Be careful when opening attachments to emails - even if the message appears to be from someone you know. Email attachments infected with viruses are one of the most widely used methods for infecting PCs.
 - Be vigilant against phishing attacks claiming financial rewards or encouraging charity donations. Phishing emails can look like they came from a real company or person you know and trust. The sole purpose of a phishing email scam is to trick you into going to a fake website that looks equally authentic and inputting personal information that would in turn provide the criminal with access to your accounts.
 - Remember that text, music and other content on the internet are copyright works. You should not download or email such content to others unless certain that the owner of such works allows this.
- Ensure not to give out your personal details, such as a mobile phone number and personal email address to learners. Do not use personal email accounts or numbers for work use.
- Ensure you keep your own shared area and own email accounts organised. Do not keep emails or documents for longer than you need and it is each individual's responsibility to ensure their accounts are organised appropriately.

General Guidance for Staff and Learners

When setting up for a video conference there are a few things you should consider.

Internet Connection

- Is it fast enough for video or should you only use audio? Typically, you need a minimum of 3Mbps upload and download for a video conference, Wi-Fi will introduce extra lag so make sure you have the best connection possible.
- Is it shared, could someone else suddenly start using a large amount of bandwidth?
- Is it reliable, could it stop working part way through your call? This mostly applies to Wi-Fi connections.

Location

- With the camera on what can be seen behind me?
- Is the light too bright / in my face / over my shoulder? All of these can make it hard for others to see you clearly.
- What is the sound like, is there background noise, does the area echo?

Others

- Confirm the nature of the video conference, if it is confidential, ask all attendees to confirm that they have taken steps to ensure confidentiality.
- Are other people in the house, children, pets that could make an unscheduled appearance. You should make them aware you are on video conference and if possible, have the room to yourself.

Best Practices - General

Thanks to the similar features in both Zoom and MS Teams the below suggestions are possible on each platform.

Background filters

It is recommended if you are video conferencing in a busy area or from home you use a static background image from the inbuilt libraries of each app. This will reduce distractions for others in the video chat, block out any unwanted cameos and protect the privacy of your home.

Headsets

Though not always necessary these are recommended as they limit the exposure of the conversation taking place. Others at your location cannot hear what is being said to you and having a mic closer to your mouth means it is less likely to pick up background noise.

Screen sharing

If you need to share something on your screen with others in the video conference it is recommended you only share the application window you need to show. This means that members of the conference can only see that application and nothing else on your computer. If you need to share multiple applications it may be necessary to share your entire screen, in this case make sure your desktop is appropriate, you may not want others to see what applications you have installed or the picture of your family on your desktop wallpaper.

Framing

Try and sit centre frame when in a chat and be aware of your movements it is easy to forget that the camera, unlike a person, cannot follow you if you move out of its field of view.

Recording Video Conferences

- Although both supported platforms have this feature it does come with considerations.
- Recording should only be used where there is a clear and justifiable reason to do so, in most cases it is recommended you check with a member of the SLT before deciding to record a session. Additional points of note are that:
 - recorded sessions are covered by GDPR and therefore, should be deleted as soon as they are no longer needed
 - anyone objecting to being recorded should be asked to leave the session, including audio only participation
 - before recording, you should plan what you are going to do with the recording afterwards, where will it be stored and for how long?
 - recordings must be deleted as soon as they are no longer needed
 - the attendees should be made aware of your plans for the recording prior to commencing recording