

LSDN E-Safety Policy	
Policy No:	QC009
Management Area:	Quality & Compliance
Author:	Janet Ravensdale
First Issue Date:	May 2022
Latest Issue Date:	March 2026
Current Version Number:	3
Most Recent Review Date:	March 2026
Reviewed by:	Anerie Huisamen
Next Review Date:	March 2027
CEO Sign-off	March 2026

LSDN MISSION STATEMENT	
LSDN’s mission is to enhance the life chances, economic independence and social mobility opportunities of its service users by helping individuals to develop vocational, academic and life skills using a supportive and individualistic approach so service users can realise their fullest potential at home, in the workplace and in the community. LSDN works in partnership with its clients and local community to bring about the best possible results for each individual and their families.	
Purpose	The policy sets out guidelines and requirements for staff and students accessing LSDN IT systems whether in the centre or remotely.
Scope	The policy applies to all students and staff and all members of the LSDN community who have access to LSDN’s IT systems, both on the premises and remotely. Any user of LSDN’s IT systems must adhere to and accept the Internet and Intranet Use Policy. The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media, instant messaging, webinar and video conferencing etc.

Management Responsibility	Compliance Manager
Policy Headings	
Introduction	London Skills & Development Network (LSDN) is a not-for-profit Social Enterprise in the field of education and training services. As well as managing and delivering a range of education and training programmes, LSDN also offers a range of consultancy and capacity building support services to the education and training sector. LSDN is in the top 2% Training Providers for Learner satisfaction (National FE Choices Survey).
Description	LSDN recognises the benefits and opportunities that new technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the organisation while supporting staff and students to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. As part of our duty to safeguard students, we will do all that we can to make our students and staff stay safe online and to satisfy our wider duty of care. Definition: The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection. 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 Responsibilities The Quality Lead and Compliance Manager is responsible for maintaining this policy. The following staff are responsible for implementing the policy:
--	--

- The Safeguarding Lead is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will deliver staff development and training, record incidents, report any developments and incidents and liaise with the local authority and external agencies to promote e-safety within the College community. The Safeguarding Lead will also provide pastoral and practical support for students dealing with issues related to e-safety.
- The Education Admin Manager for incorporating e-safety into student induction.
- The teaching staff for incorporating e-safety as part of programme delivery.
- All Managers for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.
- All members of LSDN staff for staying alert to and responding appropriately to any potential or actual e-safety issue.

Security

LSDN will do all that it can to make sure the network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations to prevent accidental or malicious access of LSDN's systems and information. Digital communications, including email and internet postings, over the network, will be monitored in line with the Internet and Intranet Use Policy.

LSDN 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.

	Behaviour LSDN will ensure that all users of technologies adhere to the standard of behaviour as set out in the Internet and Intranet Use Policy. LSDN will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary procedures. Use of Images and Video The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images' rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or students. All students and staff should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. LSDN teaching staff will provide information to students on the appropriate use of images as detailed in the Internet and Intranet Use Policy. This includes photographs of students and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner. Photographs of activities on the LSDN premises should be considered carefully and have the consent of the
--	--

	Marketing department before being published. Approved photographs should not include names of individuals without consent. Education and Training With the current unlimited nature of internet access, it is impossible for LSDN to eliminate all risks for staff and students. It is our view therefore, that LSDN should support staff and students to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively. For students Students have access to e-safety e-learning modules and assessments and 16 -18 full time students will attend e-safety tutorial sessions. An area on Google Classrooms has also been set up with e- safety resources which are signposted at induction. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. Within classes, students 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. Appendix A shows E-Safety Guidelines, Appendix B shows Guidelines for Students and Appendix D shows Guidelines for students using webinar / video conferencing software. Appendix F shows Student ICT User Guide. For staff Staff will take part in mandatory Safeguarding e-safety and/ or cyber security training on an annual basis. Further resources of useful guidance and information will be
--	--

	issued to all staff following the session. Staff attendance is recorded and monitored by HR. Staff will also be asked to sign the Internet and Intranet Use Policy. Appendix A shows E- Safety Guidelines, Appendix C shows Guidelines for Staff (Digital and Social Media) and Appendix E shows Guidelines for staff using webinar / video conferencing software. Incidents and Response Where an e-safety incident is reported to LSDN this matter will be dealt with immediately and effectively. LSDN will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their tutor, Duty Manager or to the Safeguarding Lead. Where a member of staff wishes to report an incident, they must contact their line manager, HR, Duty Manager or CEO as soon as possible. Following any incident, LSDN 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.
Links to other policies	Safeguarding, Prevent, Disciplinary, Staff Handbook, Intranet and Internet Use Policy AI Learner Guide for Further Education
Policy monitoring and review arrangements	Policy is reviewed annually or as appropriate in line with legislative updates.

Appendix A - E-Safety Guidelines

- Keep your personal information private – avoid sharing personal information such as your phone number, home address or photographs with people you don't know in person and trust.
- Check whether the social media networks you use allow you to create friend lists. These lists let you manage who sees what. For example, you may only want your closest friends to see some information.
- Use private messages for people you know in person and trust; be careful of private messaging people you don't know.
- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared it in the past, CHANGE IT).
- Know how to block someone if they make you feel uncomfortable or upset.
- Learn how to save chat logs and texts so that if someone does make you uncomfortable or upset, you have evidence to report them.
- Remember to log out of a site properly after use, especially on a shared computer.
- Keep your clothes on when using webcam – images of you could end up in the wrong hands!
- Think very carefully about meeting someone face to face who you only know online – NEVER do this alone, always take a trusted adult friend along with you and/ or ensure a trusted friend knows where you are at all times, meet in a public crowded place and make sure you have made appropriate transport arrangements.

Appendix B – Guidelines for Students (Digital and Social Media)

As part of our duty of care to our students, LSDN sets out guidelines, below, for students when using social media. These guidelines are included in the student handbook and the purpose of including them here is to make staff aware of the guidelines and to encourage staff to discuss them with students.

Students should follow the guidelines below at all times:

- Do not enter into a “friends” relationship online with someone you do not know
- Do not use social media to harass, threaten, insult, defame or bully another person or entity; to violate any LSDN policy; or to engage in any unlawful act, including but not limited to gambling, identity theft or other types of fraud
- Do not access or participate in social media which insights hatred or promotes radicalisation.
- Set up privacy settings carefully, ensure you are not sharing any information that you do not want to and check these on a regular basis
- Participating in social media use as part of course activity is optional. Students may opt out at any time
- Discussions on LSDN branded social media should be appropriate and LSDN or Course related
- When posting on sites linked to LSDN or when mentioning or referring to LSDN on social media do not:
 - Use foul or abusive language
 - Harass, threaten, insult, defame, blackmail or bully another person
 - Refer to any other member of the LSDN community, whether student or staff, in a derogatory or insulting manner
 - Refer to LSDN, its courses or facilities or any other aspect of its offering, in a derogatory or insulting manner
 - Post or comment in any way that reflects poorly on LSDN or is deemed to interfere with the conduct of LSDN business
- Posting of messages that are deemed inappropriate will be dealt with under the student disciplinary procedure
- Copies of inappropriate posts may be reported to parents/guardians and the appropriate authorities. Before you post a message, think carefully about its content and ask yourself how you would feel if you received that message or know that it may be disclosed in court

- Any form of abuse or cyber-bullying will be dealt with under the student disciplinary procedure.

Appendix C – Guidelines for Staff (Digital and Social Media)

This policy sets out guidelines for staff, below, for the use of digital and social media including emails and text messaging. These guidelines apply to: Posting to any LSDN social media site; communicating with members of the LSDN community including staff or students; discussing LSDN on any site; whether at work and using the LSDN network and equipment or through a personal account or using a personal phone, computer or other device from any other location.

Staff should always follow the guidelines below:

- Be professional; as a LSDN employee you are an ambassador for the organisation. Protect the LSDN brand and values at all times, do not make derogatory comments about LSDN products, services, management, employees or systems.
- Never have a “friend” relationship with a student online, where personal details are shared.
- If the Digital and Social Media requires a login, create a separate “work” login and ensure any privacy settings are set appropriately so that no personal information can be viewed.
- Staff should not share any personal information online including home address, personal telephone numbers, personal email addresses or date of birth.
- Discussions on social media sites linked to LSDN should be appropriate and be work or Course related.
- When communicating with students who are under 18 via email, where possible, LSDN student email addresses should be used.
- Email communications with students under 18 must happen within normal working hours (8.30 – 5pm).
- Staff should not comment on anything related to legal matters, litigation, or any parties LSDN may be in dispute with or anything that may be considered a crisis situation.
- Do not access or participate in social media which incites hatred or promotes radicalisation.
- Do not upload to video/photo sharing sites (e.g. YouTube) unless it is done via the LSDN official channel.
- Do not post a person’s photograph or video image without first obtaining permission and signed release forms from anyone depicted in the photograph or video (any photographs of children and young people under the age of 16 should have parental permission). Blank release forms may be requested from the Student Services team and should be promptly returned after they are signed.
- Protect confidential and sensitive information at all times.
- Remember that statutory regulations and LSDN policies including inappropriate conduct such as sexual (or other) harassment, bullying,

discrimination, defamation, infringement of copyright and trademark rights, data protection and unauthorised disclosure of student records and other confidential and private information, will apply to communications by LSDN students and staff through social media.

- When posting on sites linked to LSDN or when mentioning or referring to LSDN on social media do not:
 - Use foul or abusive language
 - Harass, threaten, insult, defame or bully another person
 - Refer to any other member of the LSDN community, whether student or staff, in a derogatory or insulting manner
 - Refer to LSDN, its courses or facilities or any other aspect of its offering, in a derogatory or insulting manner
 - Post or comment in any way that reflects poorly on LSDN or is deemed to interfere with the conduct of LSDN business
- Staff should not spend an excessive amount of time while at work using social media websites in a personal capacity. They should ensure that use of social media does not interfere with their other duties as this is likely to have a detrimental effect on productivity
- Any breach in this Policy could result in an investigation and disciplinary procedures under the staff disciplinary policy. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing reputational damage to LSDN, may constitute gross misconduct and lead to dismissal.

Appendix D – Guidelines for students using webinar / video conferencing software

This policy sets out guidelines for students using webinar/video conferencing software:

Do:

- Conduct yourself in a professional manner throughout calls with tutors, support staff or other students.
- Attend video calls from a desk or other appropriate location. If you do work from your bedroom, you should blur your background.
- Make sure you are dressed appropriately.
- Be punctual and courteous. Language must be professional and appropriate. Turn your phone to silent. Treat this just like you would a lesson or meeting at LSDN.
- Look at your screen, pay attention to others and when speaking make sure to look at your camera.
- Use the 'blur background option' to hide any background if needed.
- Check what you can see when you first log in as this is what others will see.
- Mute your microphone when not needing to talk to avoid any background noise.
- Position yourself away from where your family members or pets are.
- Only post chat messages relevant to the lessons.

Don't:

- Conduct/attend a video call if it would be improper for a face-to-face meeting.
- Multi-task; the tutor will be aware.
- Shout; the other participants will tell you if they cannot hear.
- Click your pen, tap on your desk or anything else annoying or distracting.
- Smoke or vape.
- Eat or drink, other than water / tea / coffee
- Leave multiple applications open during the call as it may affect the quality.

Appendix E – Guidelines for staff using webinar / video conferencing software

This policy sets out guidelines for staff using webinar/video conferencing software:

Do:

- All 1:1 online activity with under 18s or vulnerable adults **MUST** be agreed with students prior to the 1:1 taking place. The 1:1 must then take place only at the days / times agreed.
- **If at any time you feel uncomfortable during a 1:1 call, with something done or said, you should end the call as soon as possible and report any concerns to your line manager and / or safeguarding.** Examples may include: student inappropriately dressed or in an inappropriate location (e.g. bedroom).
- Please note: If your safeguarding training is not up to date you **MUST NOT** conduct a 1:1 video conferencing session. Refer to your line manager for further guidance.
- Where possible set up online meetings/lessons with students through Google Meet or Zoom and use the waiting rooms facility. This prevents unwanted guests and avoids 'Zoom Bombing'.
- Encourage students to maintain an awareness of employability skills in how they conduct themselves in online sessions.
- Conduct yourself in a professional manner throughout calls with colleagues or students - you remain an employee of LSDN throughout the call.
- Conduct video calls to students or colleagues from a desk or other appropriate location. If you do work from your bedroom, you **MUST** blur your background.
- Remind students that all calls/videos may be recorded - this is to safeguard both parties and wouldn't routinely be shared.
- Be punctual and courteous. Language must be professional and appropriate. Introduce yourself and take note of other attendees' so you can address them by name. Turn your phone to silent. Treat this just like you would a face-to-face meeting with a student, colleague or other adult.
- Test your audio and/or video before a scheduled call.
- Look at your screen, pay attention to others and when speaking make sure to look at your camera.
- Use the 'blur background option' to hide any background if needed.
- Check what you can see when you first log in as this is what others will see.
- Mute your microphone when not needing to talk to avoid any background noise.
- Position yourself away from where your children, spouse, or pets

are.

Don't:

- Conduct a video call if it would be improper for a face-to-face meeting.
 - Multi-task; your audience will be aware.
 - Shout; the other participants will tell you if they cannot hear.
 - Click your pen, tap on your desk or anything else annoying or distracting.
 - Smoke or vape.
 - Eat or drink, other than water / tea / coffee.
 - Leave multiple applications open during the call as it may affect the quality.
- Wear stripes or heavy patterns creating pixilation of images.

Appendix F – Student ICT Rules

All students are encouraged to make full use of the ICT and Internet resources available at LSDN. For everyone's protection LSDN requires that students agree to the following in order to use the computer system.

- **I will only** use ICT system at LSDN, including internet, email, digital video, mobile technologies, etc. for the purposes intended and allowed by LSDN as follows:
 - ✓ Course/learning programme
 - ✓ Employment readiness
 - ✓ Enrichment and professional development activities
- **I will not** download or install software on LSDN technologies or equipment.
- **I will only** log on to the LSDN network/Learning Platform with my own username and password.
- **I will follow** LSDN's ICT security system and not reveal my password to anyone and change my passwords regularly.
- **I will make** sure that all ICT communications with LSDN students, staff or others is considerate and responsible and does not breach LSDN centre values and LSDN Student Code of Conduct.
- **I will be** responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- **I will not** deliberately browse, download, upload or forward material that could be considered offensive or illegal. This includes any discriminatory or extremist views.
- **I will not** give out any personal information of LSDN students or staff such as name, phone number or address without their express permission to do so. I will consider principles of online safety before giving my own personal details to anyone and will take care to safeguard my password and financial information.
- **I understand** that images of LSDN students and staff will only be taken, stored and used for LSDN purposes in line with LSDN policies and procedures and will not be distributed externally without the individual's permission.
- **I will** ensure that my online activity, both at LSDN and outside LSDN, will not cause LSDN, the staff, students or others distress or bring LSDN

into disrepute.

- **I will** respect the privacy and ownership of others' work online at all times.
- **I will not** attempt to bypass the internet filtering system.
- **I understand** that my use of the Internet and other related technologies can be monitored and logged and can be made available to LSDN staff supporting the delivery and management of my course/learning programme.
- **I understand** that these rules are designed to keep LSDN students and staff safe and if they are not followed LSDN sanctions will be applied.

Appendix G – AI Learner Guide

In line with [DfE Guidelines](#), [UK Bridge AI skills guidance](#)

Artificial Intelligence (AI)

Artificial intelligence (AI) doesn't have just one definition that everyone agrees on. In simple terms however think of it as a computer system doing jobs that usually require human intelligence. Most of the time, these AI systems learn and get smarter by themselves, which is called machine learning.

Generative AI

This is a specific type of AI that can generate content like text, pictures, or computer code. It learns from large data models and generates something new based on a user's input.

Some examples of these tools are:

- **Text Generators:** Like ChatGPT or Microsoft Copilot, which can write text almost like a human.
- **Image Creators:** Such as DALL-E, which can make pictures from descriptions.
- **Coding Helpers:** Like GitHub Copilot, which suggests code while you're programming

Using AI:

Always strive to be original in your work, ensuring that what you produce is genuinely yours, even when utilising AI tools. AI should be used as a study aid, assisting in generating ideas, organising notes, explaining difficult concepts, and checking spelling and grammar. However, it's crucial to use AI with care, as it can sometimes be inaccurate and may make mistakes. Always make sure to double-check the work generated by AI to ensure accuracy and reliability.

Limitations of AI:

It is important to recognise that AI does not 'understand' its output in the same way humans do. While AI-generated content often appears plausible, it can be factually inaccurate. AI can make errors and even make information up.

Below are some limitations of AI that you should be aware of:

- **Lack of true understanding:** AI does not possess a human-like understanding of its outputs. It processes information based on algorithms and data, lacking real comprehension. For example, AI might generate a text about a medical procedure without truly understanding the complexities and implications of medical practice.

- **Potential for inaccuracies:** Despite often producing plausible results, the information can be incorrect, include errors or even be fabricated. An example of this could be AI generating some text on a historical event like the moon landing but including factual errors such as incorrect dates or describing the technology used incorrectly.
- **Inability to provide genuine references:** AI systems are not capable of providing real references for the information they generate. AI could create a convincing article about a scientific study on the benefits of a new diet, but there would be no real studies or data to back it up and the references it generates are made up.
- **Risk of bias and stereotypes:** AI can accidentally reflect and propagate stereotypes and biases in its outputs. It can for example assume that a nurse is female based on stereotypical data that the models are trained on.

How 'NOT TO USE' AI:

AI should be used as an aid, not as a replacement for a learner's own work. Misusing AI can lead to academic consequences.

Examples of how not to use AI include:

- **Submitting AI-generated work as your own:** Using AI to complete assignments, essays, or projects without proper references to tools you have used or in violation of academic guidelines is unethical and can be considered plagiarism.
- **Relying solely on AI for Learning:** Using AI as the only source of information or understanding in your studies can hinder your ability to think critically and learn deeply.
- **Bypassing learning opportunities:** Using AI to avoid engaging with challenging learning material or to bypass learning processes decreases your opportunity to develop essential skills and knowledge.
- **Ignoring the limitation of AI:** Overestimating the capabilities of AI and not checking the accuracy of its outputs can lead to the spread of incorrect or misleading information.

Guidelines for using AI in assignments:

Referencing AI

When using AI-generated content in your assignments, it's important to reference it properly. This ensures academic integrity and makes clear the extent of AI involvement in your work.

Here's how you can do it:

- **Clearly indicate AI contributions:** If your assignment includes content generated or assisted by AI, such as a text or an image, make sure to clearly indicate which parts were aided by AI. This

could be done through footnotes, endnotes, or in-text citations.

- **Provide details about the AI tool:** Include the name of the AI tool (e.g., ChatGPT, DALL-E, GitHub Copilot) and the version if applicable. This information gives context to the nature of the AI's involvement.
- **Explain the role of AI:** Briefly describe how the AI was used. For example, if AI was used for initial brainstorming, drafting, or providing a structure for your work, specify this in your reference.
- **Document AI interactions for review:** Retain a non-editable record (such as a screenshot) of the AI interaction, including the questions asked and the responses received. This documentation should be submitted along with your assignment, allowing assessors to review both the AI-generated content and its application in your work.
- **Acknowledge AI like you would a normal reference:** Recognise the use of AI tools in your assignment in a manner that upholds academic integrity. This includes precise referencing of AI sources, not just a general mention of 'AI' or 'ChatGPT'.

Academic Misconduct:

Learners are reminded to uphold academic integrity when submitting assignments. This includes ensuring that all submitted work is their own and that they adhere to LSDN's Malpractice Procedure.

AI Safety and Data Privacy

You must be conscious of the fact that AI systems, such as chatbots and image generators, can store and process the data provided to them, ranging from basic inquiries to more personal details.

To maintain privacy and security, it is advised that you:

- **Don't share sensitive information:** Avoid entering personal, financial, or confidential information into AI tools and steer clear of prompts that might require disclosing such details.
- **Be informed about data policies:** Familiarise yourself with the data collection and usage policies of various AI platforms, helping you understand the potential use or sharing of your data.
- **Exercise caution with college data:** In projects or research that involve LSDN data, always comply with LSDN's policies on data privacy and security.
- **Report any issues promptly:** Should you encounter problems related to data misuse or privacy breaches in AI usage, report these incidents immediately to a member of staff.
- **Be aware of age requirements:** Most AI tools, including ChatGPT and Microsoft Copilot, require parental consent if you are under 18, so make sure you ask your parent or guardian before using these tools.