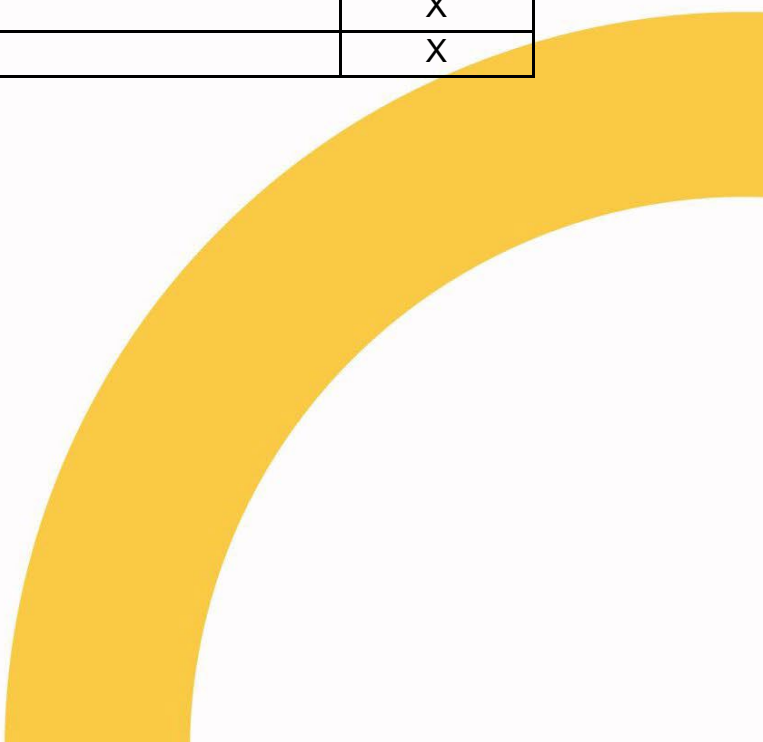


STUDENT IT ACCEPTABLE USE POLICY 2024 - 2027

APPROVED BY (SELT) ON (January 2025)

| Applies to: | |
|--|---|
| Harrogate College | X |
| Keighley College | X |
| Leeds City College | X |
| Leeds Conservatoire | X |
| Leeds Sixth Form College / Pudsey Sixth Form College | X |
| Luminate Group Services | X |
| University Centre Leeds | X |



CHANGE CONTROL

| | | |
|--|--|----------------|
| Version: | 1.2 | |
| Approval route | | |
| Approval committee (ELT, SELT, Board) | Date approved | Version |
| SELT | August 2024 | |
| SELT (amends) | January 2025 | |
| | | |
| | | |
| | | |
| Name of author: | Graham Eland | |
| Name of responsible committee: | SELT | |
| Related policies: (list) | Student Disciplinary Policy Safeguarding Policy Data Protection Policy | |
| Equality impact assessment completed | Date: | |
| | Assessment type <input checked="" type="checkbox"/> Full <input type="checkbox"/> Part <input type="checkbox"/> Not required | |
| Environmental Impact Assessment Completed | Date: | |
| | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not required | |
| Policy will be communicated via: | Policy portal and CECIL | |
| Next review date: | 3 years August 2027 | |

CONTENTS

Policy Aims and Objectives

Compliance with the IT Policy Framework

What is Mandatory and What is Advisory/Guidance?

3.1 Mandatory

3.2 Advisory/Guidance

Acceptable Use Principles and Practices

4.1 Communication with Students

4.2 Unacceptable Use

Computer Use – What Are My Responsibilities

5.1 Staff Responsibilities

Manager Responsibilities

ITSS Department Responsibilities

JISC Internet Acceptable Use – Staff Responsibilities

JISC Unacceptable Use – Staff Responsibilities

9.1 Unlawful Examples

10. What is Illegal or Harmful Use?

11. What is Hacking or Disruptive Activity?

12. Prevent (Due regard to the need to prevent staff from being drawn into terrorism)

13. Prevent Duty (Reducing permissive environments)

14. Keeping Children Safe in Education

15. Mobile and Smart Technology Unacceptable Use

16. Deepfake Technology Unacceptable Use

1. Policy Aims and Objectives

The policy defines a set of mandatory expectations for students when using computer devices and electronic communications in Luminate Education Group (the group). The primary purpose of the policy is to encourage everyone to achieve acceptable standards of use and conduct. The policy includes advice and guidance for students to support the effective use of computer devices and electronic communications. The policy also identifies the acceptable use requirements from the Prevent Duty and reducing permissible environments, the Keeping Children Safe in Education (KCSIE) statutory guidance and the acceptable use of mobile smartphones.

2. Compliance with the IT Policy Framework

It is in everyone's interest to maintain the security of the group information and IT assets. You have a responsibility to support this by protecting the security of your own data/information and to not access other people's personal systems or information.

You will be held accountable for non-compliance with the policy. Any breaches of the mandatory policy will be considered in accordance with the Student Disciplinary Policy.

To ensure students are aware of their responsibilities regarding the use/misuse of IT, this policy outlines the expected standards of use, including the following: computer use, mobile technology use, illegal or harmful use, email use and hacking.

3. What is Mandatory and What is Advisory/Guidance?

We have used two headings to describe the relative importance of each section of the policy to confirm what is expected of you and the consequences of non compliance.

3.1 Mandatory

This is important to us, and you must comply with the policy.

3.2 Advisory/Guidance

This is recommended good practice and should help you in using the computer devices and electronic communications in the most effective and efficient way.

We use the student user logon name to track system activity in audit trails. This makes all actions performed on the group systems attributable to an individual user. Where actions are inappropriate (e.g. hacking), the ITSS Department will be alerted to this.

4. Acceptable Use Principles and Practices

The group IT systems are for the use of students as part of work and study and not for the purposes of operating a personal business.

You are also allowed reasonable use of the systems for non-work/study activities, as long as these fall within the limits of [acceptable use](#) of IT systems and data. You may undertake personal communications (eg [emails](#) and [Internet](#) use) as long as these do not disrupt the work/study of others or threaten the reputation of the group.

Our systems enable us to monitor telephone call date/times, e-mail, internet and other communications. For business reasons, and to ensure our legal obligations in our role as a learning organisation, use of our systems including the telephone and computer systems and any personal use of them, is continually monitored by use of automated software and filtering

services. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for the group legitimate interests.

The contents of our IT resources and communications systems are the property of the group. Students should have no expectation of privacy in any message, files, data, document, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review, without further notice, student activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate interests of the data controller as a legal basis. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well other network monitoring technologies.

If the group identify any illegal or concerning activity during monitoring (for example under the Child Protection Act, Radicalisation under the PREVENT Duty or Counter- Terrorism and Security Act) you will be referred as appropriate to the Safeguarding Team for support or police for investigation.

The group takes any breach of the policy very seriously and these will be considered in accordance with the Disciplinary Policy. In serious cases, a breach may be treated as gross misconduct leading to summary dismissal.

If concerns are raised regarding alleged misuse of Internet access or email content, detailed reports can be provided. All student internet browsing is recorded against individual user accounts.

4.1 Communication with Staff and Students

Students are required in all communication to comply with the requirements of the following policies:

- Student Disciplinary Policy
- Safeguarding Policy
- Data Protection Policy

4.2 Unacceptable Use

- Publish or send personal/sensitive data including photographs of students or staff without the recorded consent of the individuals in line with GDPR requirements.
- Invite/accept your personal social media (Facebook/X, Instagram, TikTok) account with staff personal social media accounts. Do not send inappropriate messages that contravene the policy or related policies listed in this document.
- Say anything that is dishonest, untrue, or misleading. What you publish will be available on the Internet for a long time, so consider the content carefully and do not disclose personal details.
- Post any material critical of the group or colleagues on any email, website, or social media site.

- Post anything contradictory or in conflict with the group websites.
- Post comments that run counter to the Group Equality and Diversity policy.
- Post comments that recommend, or appear to endorse, law-breaking of any kind.
- Post comments that exhibit or appear to endorse behaviour that could be argued to encourage “copycat” behaviour. This would include for example, dangerous driving, alcohol or drug abuse.
- Allow staff to see/use or communicate with your own personal communication systems, for example your own personal email, Facebook/X, Instagram or TikTok accounts.
- Allow staff to see/use or communicate with your own personal mobile phone and phone number.
- Participate in using “spyware” software and other illegal forms of snooping software.
- Reference any confidential information about customers, partners or suppliers without their consent in line with GDPR legislation.
- Post comments that promote extremism or radicalisation.

5.Computer Use - What Are My Responsibilities?

To ensure clarity of what the group (and the law) feel is the appropriate use of our IT systems, we have set out the boundaries and definitions below. For the avoidance of doubt, this policy covers all students studying or accessing the group resources.

5.1 Student Responsibilities

- You have a responsibility to protect the security of our systems and data.
- You should only access systems and data that are needed for your work or studies. IT security controls should prevent you from accessing inappropriate systems / information.
- Students are expected to report where systems have not been set up correctly.
- If you have reasonable belief that someone else is abusing the IT systems, you have a duty to inform your tutor.

6.Teacher Responsibilities

Ensure staff are aware of the IT acceptable use policy.

7.ITSS Department Responsibilities

Providing support and advice to students where required. JISC is the academic network which links the Colleges with other College/Universities and provides internet connectivity. We all work under the JISC acceptable use policy and staff and students are bound by its rules.

There are clear policies in place for students and staff using IT equipment and networks to research terrorism and counter terrorism during their learning. Universities UK has published advice on this at <https://www.universitiesuk.ac.uk/>

8.JISC Internet Acceptable Use - Staff Responsibilities

- The group and its members may use JISC for the purpose of communicating with other user organisations and its members, and with organisations, individuals and services attached to networks which are reachable via JISC.
- JISC may be used by the group staff and students for any lawful activity. Use by its staff and students may be in pursuance of activities for commercial gain as well as for not-for-profit activities.
- It is the responsibility of the group to ensure that its staff and students use JISC services in accordance with the JISC Acceptable Use Policy and with current legislation [Acceptable Use Policy | Jisc community](#)

9.JISC Unacceptable Use - Student Responsibilities

JISC will not be used by the group or its members for any activity that may reasonably be regarded as unlawful.

9.1 Unacceptable Unlawful Examples (includes but is not limited to these activities):

- Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of material with intent to defraud.
- Creation or transmission of defamatory material.
- Creation or transmission of material such that infringes the copyright of another person.
- Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services.
- Deliberate unauthorised access to networked facilities or services.
- Deliberate unauthorised access to terrorism and counter terrorism.
- Corrupting or destroying other user data. Violating the privacy of other users.
- Disrupting the work of other users.
- Denying service to other users.
- Other misuses, such as the introduction of “viruses”, “ransomware” or other harmful software.
- Creation or transmission of any material linked to extremism or radicalisation.

10.What is Illegal or Harmful use?

You may only access and use the group internet and network (including email, blogs and social networking) for lawful purposes. You are personally responsible for any transmission you send, post, access, or store via the IT network, including the content of any communication. Examples of illegal or harmful actions that are not permitted include:

- **Copying/Stealing:** copying/stealing of material already written by another person or material protected by copyright, trademark, patent or other intellectual property rights.
- **Offensive Materials:** distributing or posting material that is unlawful, libellous, defamatory, obscene, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory or otherwise objectionable. You must not access or use our websites or IT network in any manner to send or distribute any images containing pornography.
- **Fraudulent Conduct:** offering or distributing fraudulent goods, services, schemes.
- **Failure to Abide by Third-Party Website Policies:** violating the rules, regulations, or policies that apply to any third-party network, server, computer database, or website that you access.
- **Harmful Content:** distributing or posting harmful content including viruses, Trojan horses, ransomware, or any other computer programming routines that may damage, interfere with, lock, secretly intercept or seize any system, program, data or personal information.

11.What is Hacking or Disruptive Activity?

You must not abuse the security of our websites or IT network in any way. Examples of hacking/disruptive activity

- **Hacking:** unauthorised access to or use of data, systems or IT networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security without the prior authorisation of the owner of the system and the ITSS department.
- **Interception:** unauthorised monitoring of data or traffic on any IT network or system without the prior authorisation of the owner of the system and the ITSS Department.
- **Intentional Interference:** interference with service to any user, host or IT network including, denial-of-service attacks, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system, and broadcast attacks.
- **Avoiding System Restrictions:** using manual or electronic means to avoid any limitations established by the group or attempting to gain unauthorised access to, alter, or destroy any information that relates to the group or other end-user.

12.Prevent (Due regard to the need to prevent staff from being drawn into terrorism)

To support the group students to meet this duty, the Department for Education has published internet filtering and monitoring standards which the group has accepted and implemented. All student internet activity is monitored.

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>

13. Prevent Duty (Reducing permissive environments)

In line with the Prevent Duty requirements, the group takes all reasonable steps to reduce permissive environments by ensuring searching and/or sharing of inappropriate content is both filtered and monitored, therefore reducing exposure to inappropriate content. The group has implemented Smoothwall internet filtering (restricts access to inappropriate websites with harmful content) and Smoothwall monitor (monitors staff and student keyboard activity and alerts designated safeguarding officers on any inappropriate keywords typed) technologies.

The Prevent Duty guidance: guidance for specified authorities in England and Wales can be accessed here [Prevent Duty](#) which identifies good practice and guidance.

14. Keeping Children Safe in Education

The group has a responsibility for keeping children safe in education (KCSIE) which includes internet filtering. Appropriate filtering and monitoring technology is in place described in section 13 of the following document. Staff and students are aware of this and their roles and responsibilities.

https://assets.publishing.service.gov.uk/media/64f0a68ea78c5f000dc6f3b2/Keeping_children_safe_in_education_2023.pdf

15. Mobile and Smart Technology Unacceptable Use

Many staff and students have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). It is understood students could sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

The breadth of issues classified within online safety is considerable and continually evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Any staff or students within the group campuses using their personal smart phone including (3G, 4G or 5G connectivity) or a group issued smart phone are personally

responsible for any transmission sent, posted, accessed or stored including the content of any communication.

If you identify students at risk, please report it to the correct internal contact and the Anti-Phishing Working Group <https://apwg.org>

16. Deepfake Technology Unacceptable Use

Deepfake technology are images, videos or audio which are edited or generated using artificial intelligence (AI) tools to present false results. The image or video created by AI merges events, or characters that didn't actually happen.

A popular example of a deepfake is an image / video with someone's face technically swapped onto a different persons body, possibly with a third persons voice, therefore presenting a false character.

Deepfakes have stormed the Internet is now linked not only to innocent videos and swapping faces, it's also associated with misinformation, propaganda particularly in politics, pornography and cyber attacks.

Any creation, use or presentation of deepfake images or videos to be used negatively or in a false environment is unacceptable.