Online Safety Policy

Ratification Date: ___20/07/21_____

Signed: ___AJHawkins_____

Review Date: ___11/09/26_____

Date of next review: September 27

Version Control

Version	Date	Changes
1		Original
	July 23	Initial Review
1.1	Sept 23	Language changes for consistency. Pupils to students, and co-ordinator to lead.
		Sentence added re use of personal devices for taking photos. Use of personal devices is not permitted. All mobile phones must be turned off or on silent during lesson times and must not be used. Any breaches will be dealt with using the provision's behaviour policy.
2	26/09/24	Policy amended – Section 6 new policy on no mobile phones; references to FSC removed
	12/09/25	Reviewed, no amends
3	04/09/26	Staff Awarenes, point 1-Explanation of AUP added (Acceptable use Policy). Data storage-final sentence reworded. Social Networking Sites, points 1,2 and 3-reworded. Digital Images, point 3-reworded. Digital Images-last word in final sentence changed to 'them'.
3.1	11/09/26	Added requirements for LGfL firewall and filtering, safeguarding review of monitoring reports, and the safe and responsible use of artificial intelligence (AI).

Review

Approved and reviewed by The Board of Directors.

This policy will be reviewed annually, or more frequently, if necessary, to ensure that it remains up-to-date and effective. The review will take into account changes in legislation, guidance, and best practice.

Role	Name
Provision COO.	Dave Smith
Provision CEO	Andy Hawkins

1. Rationale

It is the duty of Liminal to ensure that every student in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, students are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy for staff, directors, visitors and students, is to protect the interests and safety of the whole provision community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following provision policies: Child Protection, Health and Safety and Behaviour.

Both this policy and the Acceptable Use Policies (for all staff, directors, visitors and students) are inclusive of both fixed and mobile internet, technologies provided by the provision (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by students or staff.

2. The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information.

Current and emerging technologies used in provision and, more importantly in many cases, used outside of provision by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

3. Whole provision Approach to the Safe use of ICT

Creating a safe ICT learning environment includes three main elements in Liminal:

1\. An effective range of technological tools which are filtered and monitored;

2\. Policies and procedures, with clear roles and responsibilities;

3\. A comprehensive e-Safety education programme for students, staff and parents.

4. Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Liminal and the COO, with the support of the Board of Directors, aims to embed safe practices into the culture of

Liminal. The COO ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

The responsibility for e-Safety has been designated to a member of the senior leadership team.

Our provision e-Safety lead is Dave Smith

Our e-Safety lead ensures he keeps up to date with e-Safety issues and guidance through organisations such as The Child Exploitation and Online Protection (CEOP). The provision's e-Safety lead ensures the CEO, Senior Management and directors are updated as necessary.

Staff awareness

All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.

- New staff receive information on the provision's AUP (Acceptable Use Policy) as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the provision community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-safety records of concern are completed by staff as soon as incidents occur and are reported directly to the provision's designated safeguarding team.

All staff working with students are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following provision e-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in provision.

5.Internet:

- The provision's internet connection is protected by the LGfL firewall and SchoolProtect filtering and monitoring services. Appropriate filtering policies will be applied to staff and student accounts and devices to minimise access to harmful, illegal or inappropriate content.
- The filtering system will be configured and reviewed according to the age and needs of students, while ensuring that it does not unreasonably restrict teaching, learning or access to safeguarding information.
- Requests to allow or block websites must be submitted to an authorised member of staff. Changes will only be made following an assessment of educational need, safeguarding risk and data protection considerations.
- Staff must not attempt to bypass the LGfL firewall, web filtering, monitoring controls or network security. Students must not use proxy websites, virtual private networks (VPNs), personal hotspots or other methods to avoid the provision's controls.
- Filtering and monitoring alerts, reports and trends will be reviewed regularly by authorised staff. Any concern indicating possible harm, exploitation, radicalisation, self-harm, abuse, bullying or other safeguarding risk must be reported promptly to the Designated Safeguarding Lead (DSL), in accordance with the Child Protection Policy.
- Urgent or high-risk alerts must be passed to the DSL immediately. Relevant information will be recorded on the provision's safeguarding system, and access to filtering and monitoring reports will be limited to staff who require it for their role.

- Staff, students and visitors have access to the internet through the provision's fixed and mobile internet technology.
- Staff should email provision-related information using their provision account and not their personal accounts.
- Staff will preview any websites before recommending to students.
- Internet searches are conducted using the Safe Search homepage found at http\://www\.safesearchkids.com/.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- If staff or students discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety lead detailing the device and username.
- Staff and students are aware that provision based email and internet activity is monitored and can be explored further if required.
- Students using the World Wide Web are expected not to deliberately seek out offensive materials. Should any students encounter any such material accidentally, they are expected to report it immediately to a teacher who will notify the E-safety lead.
- Students are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.
- They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved provision project.
- Students consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the provision's behaviour policy.
- Students will be asked to sign to the Acceptable Use Agreement thus ensuring that they are aware of expectations. Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

6.Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.
- Mobile technology for pupil use, such as iPads and netbooks, are stored in a locked cupboard. Access is available via the provision office or keyholders.

Members of provision staff (not visitors or children) should sign in/out the technologies before and after each use.

- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- Personal devices must not be used to take pictures or videos of students
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff or students are to be used during learning time. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent.

Students - Liminal Education has a "no personal mobile phone/device" approach in terms of learning.

- If students bring in mobile phones/devices, they must be handed in to staff at the start of the day. They will be returned to students at the end of the day.
- Unless express permission is given by a member of staff to do so, mobile phones cannot be used at any time during the day . Any student not following these rules will be dealt with using the provision's Behaviour policy.
- Similarly if a student refuses to hand in their mobile device they will be refused entry to the provision and dealt with using the Behaviour Policy.

7.Data storage

Staff are expected to save all data relating to their work to their Laptop if they have been assigned one or to the Google Drive Account.

The provision discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside provision or sent by post or courier.

Staff laptops should be encrypted if any data or passwords are stored on them.

ILPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks.

Staff must only take offsite information they are authorised to and only when it is necessary and required in order to fulfil their role. If a member of staff is unsure, they should speak to a member of the provision Management Team.

8.Social Networking Sites

- The use of such sites should be done with extreme caution, staff should be aware of the nature of what they are publishing on-line in relation to their professional position. Staff should not publish any information online which they would not want their employer to see.
- Under no circumstances should students or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Staff's role in Liminal requires a high degree of professionalism and confidentiality.
- Any communications or content a member of staff publishes that causes damage to Liminal, partner organisations any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the Liminal Dismissal and Disciplinary Policies apply. This could also undermine any complaints procedures.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- Liminal expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not be done either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring Liminal into disrepute;
- breach confidentiality;
- breach copyright;

- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example

by:

- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting images that are discriminatory or offensive or links to such
- content.

Liminal reserves the right to monitor staff internet usage. The Service considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

9.Digital images

- Use only digital cameras and video cameras provided by the provision and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children unless prior authorisation has been provided.
- If it is used in this way then images must be removed before leaving the provision premises.
- Ensure you are aware of the students whose parents/guardians have not given permission for their child's image to be used in provision. Up to date records of permissions are kept in student files.
- When using student's images for any provision activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against them.

10.Providing a comprehensive E-safety education to students and parents

- All staff working with children must share a collective responsibility to provide e-safety education to pupils and to promote e-safety in their own actions.
- Formally, an e-safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Even if e- safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum.
- Informally, a talking culture is encouraged in classrooms which allows esafety issues to be addressed as and when they arise.
- The ICT lead will lead regular e-safety events, including on Safer Internet Day, highlighting relevant e-safety issues and promoting safe use of technologies.
- e-Safety themes are also woven into the fabric of the Liminal curriculum.
- When children use provision computers, staff should make sure children are fully aware of the agreement they are making to follow the provision's ICT guidelines.

11. Artificial Intelligence (AI)

Liminal recognises that generative artificial intelligence tools can support education and administration when used safely, ethically and with appropriate professional oversight.

- Only AI tools approved by Liminal may be used for provision business or with students. Staff must follow the terms of use and age restrictions of each service.

- Staff and students must not enter personal data, special-category data, safeguarding information, confidential records, assessment information or identifiable images into public AI tools.
- AI-generated content must be checked by a responsible person for accuracy, bias, suitability, copyright and potential harm before it is used or shared. AI output must not be treated as automatically reliable.
- Staff remain professionally responsible for decisions, communications, learning materials and records produced with the assistance of AI. AI must not make final safeguarding, behaviour, admissions, assessment or other significant decisions about an individual.
- Students must use AI only when authorised and must follow staff instructions. They must not use AI to bully, impersonate, deceive, create harmful or sexualised content, bypass learning, or submit AI-generated work as their own.
- Where AI use is permitted in assessed or submitted work, students must acknowledge that use in the manner directed by staff. Suspected misuse will be managed in line with the Behaviour Policy and any applicable awarding-body rules.
- Any AI-generated content or interaction that raises a safeguarding concern, including harmful advice, grooming, exploitation, deepfakes or inappropriate generated images, must be preserved where safe to do so and reported immediately to the DSL.
- Liminal will include safe and responsible AI use within staff training and student online-safety education and will review approved tools as technology and guidance develop.

12. Maintaining the security of the provision IT Network

Liminal maintains the security of the provision network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network Complaints procedure.

As with other areas of the provision, if a member of staff, a child or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the e-safety lead in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern will be recorded using a Notice of Concern proforma and reported to the provision's designated safeguarding lead in accordance with provision's child protection policy. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

13. Monitoring

The CEO/COO or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the provision at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain provision business related information; to confirm or investigate compliance with Liminal policies, standards and procedures, to ensure the effective operation of provision ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Authorised staff will review LGfL/SchoolProtect filtering and monitoring reports at an appropriate frequency and record significant actions. Reports will be used to identify individual concerns and wider patterns. Any information that may indicate a safeguarding concern will be shared promptly

with the DSL. Monitoring will be proportionate, handled confidentially and undertaken in accordance with data protection law and the provision's safeguarding responsibilities.

14.Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the Liminal Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

15.Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the e-Safety lead. Where an incident involves or may involve a risk of harm to a child, it must also be reported immediately to the Designated Safeguarding Lead and recorded in accordance with the Child Protection Policy. Relevant evidence, including URLs, usernames, dates, times, screenshots and LGfL/SchoolProtect alerts or reports, should be preserved where it is safe and lawful to do so. Staff must not investigate a safeguarding concern beyond what is necessary to establish the immediate facts and protect the student.