Online Safety Policy

Author: Pilar Canal
Date: December 2022

Next Review Date: December 2023

Introduction

New technologies have become integral to the lives of young people in today's world. The internet and other digital information and communications technologies are powerful tools, which offer new opportunities for everyone. LMI College strongly believes in the educational value of technology and recognizes its potential to support and enhance curriculum. Technologies have enormous benefits: stimulating discussion, promoting creativity, enabling connectivity and enhancing learning. At home, technology is changing the way young people live and manage their time as well as the activities in which they choose to engage. These trends are set to continue.

LMI college authorizes students to use technology owned or otherwise provided by the school as necessary for instructional purposes. The use of technology is a privilege and is subject to the conditions and restrictions set forth in this document,

The school reserves the right to suspend access at any time when rules and regulations are nor being followed, or when the integrity of any member of the school is affected.

1.1 **Potential dangers and risk in the use of technology:**

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data
- The risk of being subject to grooming by those with whom contact has been made online
- The risk of coming into contact with extremist material posted with the aim of radicalisation
- The sharing / distribution of personal images without consent or knowledge ● Inappropriate contact / communication with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information, particularly with regard to concerns about 'fake news'
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and/or learning.

2. Aims of the Policy

2.1 The aims of the Digital Safety policy are to:

● promote the welfare and safeguarding of students and staff at the School ● ensure that students are ICT literate and can use the relevant facilities to ensure that their educational provision is enhanced to the maximum

- promote responsible and effective use of electronic communication (including the use of the internet, social media, mobile phones and digital technology)
- educate students and staff about the risks, responsibilities and potential criminal implications involved in the use of technology
- raise awareness of and counter instances of cyber-bullying, including bullying via text message, instant-messenger services and social network sites (such as Facebook, Twitter, Instagram, SnapChat, etc.), email, and images or videos posted on the internet or spread via mobile phones

3. Management of the Policy

3.1 This Policy has been written by the School and builds on the recommended European and UK government guidance. The following measures are in place to support this policy:

- The induction of new students and staff
- Regular training for all staff
- Guidance during any academic lesson about use of the internet
- Specific guidance to exam classes about plagiarism

4. Access to the Internet

The School will do all it can to monitor access to the internet via the School network.

Student Expectations

LMI College expects all students to use technology responsibly in order to avoid potential problems and liability. The school may place reasonable restrictions on the sites, material, and/or information that students may access through the system.

Student Obligations and Responsibilities

Students are expected to use technology safely, responsibly, and for educational purposes only. Students shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned. Students are prohibited from using technology for improper purposes, including, but not limited to, use of technology to:

- Access, post, display, or otherwise use material that is discriminatory, libelous, obscene, sexually explicit, or disruptive;
- Bully, harass, intimidate, or threaten other students, staff, or other individuals ("cyberbullying");
- Disclose, use, or disseminate personal identification information (such as name, address, telephone number, Social Security number, or other personal information) of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person;
- Infringe on copyright, license, trademark, patent, or other intellectual property rights;
- Intentionally disrupt or harm school technology or other school operations (such as destroying school equipment, placing a virus on school computers, adding or removing a computer program without permission from teacher or other school personnel, changing settings on shared computers);
- Share access information for online learning platforms or meetings with unauthorized users, or otherwise disrupt
  computer-based distance learning modules (e.g. “zoombombing”);
- Audio or video record school staff or students without the express written consent of the school;
- When using a school-provided internet connection, including a school-provided hotspot, maintain acceptable bandwidth and data use;
- Install unauthorized software;
- Unauthorized access into the system to manipulate data of the school or other users; and/or
- Engage in or promote any practice that is unethical or violates any law or school policy, administrative regulation, or school practice.

Personally Owned Devices

If a student uses a personally owned device to access LMI technology, he/she shall abide by all applicable policies, administrative regulations, and this document. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

Reporting

If a student becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of the internet services or devices , he/she shall immediately report such information to the teacher or other staff member.

Students and staff are granted access to the internet by agreeing to the terms of the relevant Acceptable Use Policy. Any student or member of staff who breaches these terms may have access

to the internet withdrawn.

The School will ensure that guidance about the copying and subsequent use of internet-derived materials by students and staff complies with copyright law, and students will be taught to be critically aware of the materials they read. They will also be taught to acknowledge the sources of information used.

The security of the School information systems will be reviewed regularly with eSecurity measures updated on a regular basis.

5. Email

Students and staff are inducted into the appropriate use of email and there is clear guidance as follows:

- School email address and drive is to be used for educational purposes only.
- The email address provided by the school to each student is the property of LMI college.
- If a child receives any inappropriate emails, he/she should inform class teacher and a parent/guardian.
- Students will use approved class email accounts in school under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers, pictures or passwords.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students will not have access to chat rooms, discussion forums, messaging or other electronic communication forums.

Transparency, openness and appropriate professional purpose must underpin all academic interaction with students via electronic and digital means.

6. Social Media

Staff are bound by the Limitless Minds International Corporation's Social Media Policy.

6.1 Students and staff should follow the following guidelines regarding the use of Social Media:

- Students and staff are advised to always keep their social media profiles on the highest levels of privacy and to update privacy settings regularly
- Students and staff are advised never to give out personal details of any kind which may enable them or their location to be identified
- Staff are advised to avoid posts or comments that refer to specific matters related to the School and / or members of its community on any social media sites, and to be mindful of their

professional reputation and the reputation of the School whilst conducting any online activity

- Staff are advised not to run social network spaces for students' use on a personal basis; any sharing of homework, lesson plans, etc. should be done via the School's internal Virtual Learning Environment / student Intranet
- Staff are advised not to allow any current student (including a recent leaver, i.e. in the school year immediately following the year of their leaving the School) to be their 'friend' or 'follower' on any social media site
- Students, staff and parents are regularly updated with advice and information concerning new social media apps, changes in social media protocols (for example Snapchat's location finder) and trends in online behaviour
- Students and staff are regularly reminded of the risks posed by adults or young people who use the internet and social media to bully, groom, abuse or radicalise other people

7. Cyber-Bullying

7.1 The internet and social networking sites must not be used to intentionally or deliberately hurt, humiliate, slander or defame another person. students are made aware that actions in this regard undertaken outside of School may also contravene School policies and so may be subject to School sanctions (in the first instance). The same sanctions will apply to incidents of cyber-bullying as would apply to any other form of bullying.

7.2 The Anti-Bullying Policy gives further guidance on cyber-bullying and a summary is displayed on the noticeboard of every classroom.

8. Sexting

8.1 In August 2016, the UK Council for Child Internet Safety (UKCCIS) published non-statutory guidance on managing incidents of sexting by under-18s. The UKCCIS guidance is non- statutory, but should be read alongside Keeping Children Safe in Education (KCSIE)5, and it should be followed unless there is a good reason not to do so.

8.2 There is no clear definition of 'sexting'. The UKCCIS guidance uses the terminology 'youth-produced sexual imagery'. This is imagery that is being created by under-18s themselves and involves still photographs, video and / or streaming. In the guidance, this content is described as sexual and not indecent. The term 'indecent' is subjective and has no specific definition in UK law.

8.3 Incidents covered by the guidance:

- A person under 18 creates a sexual image of themself and shares it with another person under 18.
- A person under 18 shares an image of another under-18 with another person under 18 or an adult.

● A person under 18 is in possession of sexual imagery created by another person under 18.

8.4 Incidents not covered by the guidance:

- Under-18s sharing adult pornography.
- Under-18s sharing sexual texts without sexual imagery.
- Adults sharing sexual imagery of under-18s. (This is child sexual abuse and must always be reported to police.)

8.5 See Appendix 1 for how to respond to incidents of youth produced sexual imagery.

9. Mobile phones and portable electronic devices

- As a commuting school in Madrid, the School believes that students must be in possession of a mobile device for the journey to and from School and in the event of any emergency or critical incident.
- Students may use mobile phones and portable electronic devices as outlined above.
- Students and staff are made aware that the guidelines that apply to the use of the School network also apply to any handheld communication device that is brought into School. Nothing that is inappropriate or potentially illegal should be downloaded or saved onto these devices, and all students and staff should be aware of the possible criminality of transmitting such material.
- Where information is accessed on personal devices, including through the device owner's service provider, whether or not such use is permitted, such devices may be confiscated and examined. The School may require staff to conduct searches of personal accounts or devices if they are suspected to have been used in contravention of this policy.

10. Photography / Video recording / Audio recording

Students and staff should follow the following guidelines regarding the use of Social Media:

● Any recording taken of a student must be for legitimate educational reasons. The validity and necessity of such a recording must be transparent, obvious and approved in advance by the member of staff's line-manager.

● Student consent must always be obtained; recordings must never be clandestine

● Care must be taken if recording images of students in clothing other than normal school dress. It is never acceptable to record images where students may not be fully dressed.

● It is best practice to use designated equipment to make or show recordings (or any other relevant material for educational purposes)

● Should staff use their own personal mobile or digital device to capture images of students for School promotional materials the following protocol must be adopted: ○ Imagery must be transferred from the device to the School network as soon as is practicable

Imagery must be deleted permanently from the device as soon as is practicable

●Copies of any recording taken of a student must not be made, nor distributed or shared

11. Complaints

All incidents of serious internet misuse must be recorded and passed on to the Principal of the school.

12. Child Protection and Safeguarding

Cyber-bullying, grooming, radicalisation and sexting are safeguarding issues. As a result, any concerns regarding students and their digital activities should be discussed with the senior leadership team or DSL before taking action.

Staff, parents and students should be aware that School email and internet usage (including through School Wi-Fi) will be monitored for Safeguarding and Conduct purposes, and both web history and school email accounts may be accessed where necessary for a lawful purpose, including serious conduct or welfare concerns, concerns regarding extremism, and for the protection of others.

Annex 1: Response to incidents of youth produced sexual imagery

Guidance from: UKCCIS Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People, 2016

1.1 The response should be guided by the 'principle of proportionality'. 'The primary concern at all times should be the welfare and protection of the young people involved.'

1.2 The Law

Making, possessing, and distributing any imagery of someone under 18 which is indecent is illegal. This includes imagery of yourself if you are under 18. 'Indecent' is not definitively defined in law, but images are likely to be considered indecent if they depict:

- a naked young person
- a topless girl
- an image which displays genitals
- sex acts including masturbation
- indecent images may also include overtly sexual images of young people in their underwear

These laws were not created to criminalise young people but to protect them. Although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. Young people need education, support, and safeguarding, not criminalisation. The National Police Chiefs' Council (NPCC) is clear that "youth-produced sexual imagery should be primarily treated as a safeguarding issue."

Schools may respond to incidents without involving the police. (However, in some circumstances, the police must always be involved.)

1.3 Crime recording

When the police are notified about youth-produced sexual imagery, they must record this as a crime. The incident is listed as a crime, and the young person is the suspect. This is, however, not the same

as a criminal record. Every crime must be reported to the police.
Schools can be assured that the police have the discretion they need not to adversely impact young people in the future.

1.4 Handling incidents

- Refer to the student's DSL
- The DSL will meet with the young person / people involved
- Do not view the image unless it is unavoidable (see Viewing Images below); confiscate the device, switch off the device and place the device in a sealed (and signed and dated) envelope.
- Discuss with parents, unless there is an issue where that's not possible
- If there is any concern the young person is at risk of harm, social care or the police should be contacted

Always refer to the police or social care if incident involves:

- an adult
- coercion, blackmail, or grooming
- concerns about capacity to consent (e.g. if the young person has SEN)
- images show atypical sexual behaviour for the child's developmental stage
- violent acts are depicted
- image shows sex acts and includes a child under 13
- a young person at risk of immediate harm as a result of the disclosure (for example, self-harm or suicide)

Once a DSL has enough information, the decision should be made to deal with the matter in school or to refer it to the police or to social care. All information and decision-making should be recorded in line with school policy. If the incident has been dealt with in school, a further review should be held to assess risks.

1.5 Assessing the risks once the images have been shared

When assessing the risks (to the young person) when an image has been shared, the following points should be considered:

- Has it been shared with the knowledge of the young person?
- Are adults involved in the sharing?
- Was there pressure to make the image?
- What is the impact on those involved?
- Does the child or children have additional vulnerabilities?
- Has the child taken part in producing sexual imagery before?

1.6 Viewing images

- Avoid viewing youth-produced sexual imagery. Instead, respond to what you have been told the image contains.
- If such imagery is viewed, discuss with the DSL immediately.

- Never copy, print, or share the image (it is illegal to do so).
- View the image with another member of staff present.
- Record the fact that the images were viewed, along with reasons for doing so and who was present. Sign and date this record.

1.7 Deleting images (from devices and social media)

If the school has decided that involving other agencies is not necessary, consideration should be given to deleting the images. It is recommended that students are asked to delete the images themselves and confirm they have done so. This should be recorded, signed, and dated. Any refusal to delete the images should be treated seriously, reminding the student that possession is unlawful.