Centre For Self Managed Learning

e-Safety Policy

POLICY DOCUMENT 11	
Title	**e-Safety Policy**
Approved by	Board of Trustees
Date approved	16 November 2023
To be reviewed	Every three years; on legislative changes; in the event of a serious incident
Review history	28 July 2020
Executive director owner	Chair of Trustees
Where to be published (website/private)	Website

Contents

1. Key Contacts

1.1 The Designated Safeguarding Lead (DSL) at SML College is Ian Cunningham. He can be reached on 01273 987629 or on by email ian@smlcollege.org.uk. If the DSL is not available, contact should be directed to the Deputy Safeguarding Lead Jessie Beagley by email jessie@smlcollege.org.uk

2. Aim, Purpose, Principles

2.1 Aims

Staff, Learning Advisors, volunteers (Stakeholders) and student have an entitlement to technology to support learning, including access to the Internet. The e-safety policy for SML College is designed to help to ensure safe and appropriate access and behaviours.

2.2 Purpose

This document has been written in order to produce clear guidelines for everyone within the SML community, including, but not limited to, staff (any-term), hired contractors (Learning Advisers), volunteers, visitors, students and any other users of Information Communication Technology (ICT). Hereinafter referred to as "Users". This policy applies to the SML College site

2.3 Principles

The appropriate use of the Internet and other technologies can extend and enhance learning. However, the use of these new technologies can put young people at risk within and outside SML College.

The Internet has the capacity to instantly connect users to content and to each other, but also presents unprecedented levels of risk to both students and adults at SML College. Equally, access to personal devices gives students access to powerful digital tools wherever they go. Some of the danger's students may face include:

- Access to illegal, harmful or inappropriate content,
- Access to content that promotes extremism and / or radicalisation,
- Losing control over personal information/ images,
- The risk of being groomed by those with whom they make contact, exposing them to physical and sexual risk
- Exposure to, or engagement in cyber-bullying,
- An over-reliance on unreliable sources of information with the possibility that they will not be able to evaluate the quality,
- Accuracy and relevance of information on the Internet,
- Plagiarism and copyright infringement exposing students to academic and legal risk

This e-safety policy explains how SML College ensures that there are reasonable safeguards to manage and reduce these risks so that technology can impact positively on learning and administration.

3. Additional Notes

Many of these risks touch on areas covered by the Safeguarding and IT Acceptable Use policies, which need to reference this E-safety policy.

SML College acknowledges that it may not be possible to eliminate all of the above risks entirely, so it is important that students' understanding of the risks to which they may be exposed is built through good educational provision, so that they have the confidence and skills to face and deal with them.

4. Adult Stakeholder Responsibilities

All adults will make themselves aware of the content of this policy and if required, will attend relevant e-safety training.

Stakeholders who use online provisions to support the learning of SML college students shall be responsible for contributing to the positive re-enforcement of e-safety behaviours through their day-to-day interaction with students and technology.

All Stakeholders will remain aware of any students' that use personal devices within the college e.g. (mobile phones, iPods) and carefully monitor if they have concerns of this usage

5. E-safety DSL

SML College will designate the Designated Safeguarding Lead to monitor E-safety. The Designated Safeguarding Lead shall;

- Co-ordinate any e-safety education programme for students, parents and governors, if required

- Ensure a record of e-safety incidents and the actions taken is maintained

- Liaise with relevant ICT Services over e-safety issues,

- Maintain an up-to-date understanding of developments in e-safety

6 Educational activities

6.1 E-safety education for students

6.1.1 Whilst regulation and technical solutions are particularly important, SML College acknowledges that their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the e-safety provision. SML college acknowledges that students will need the help and support of the college to recognise and avoid e-safety risks and build their resilience.

6.1.2 E-safety should be referenced whenever online provision is used and Stakeholders should reinforce e-safety messages whenever ICT is being used:

6.1.3 Where the Internet is accessed, it is best practice that students be guided to sites checked as suitable for their use (as identified by Stakeholders) and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

6.1.4 It is accepted that students may need to research topics (e.g. racism, drugs, discrimination) that could result in Internet searches being blocked via the online provisions provided by SML College. In such a situation, Stakeholders can request a temporary removal of those sites from the filtered list, for the period of study. Any request to do so needs to be submitted to the DSL and should be auditable, time-limited and with clear reasons given.

6.1.5 Whenever the Internet is used for research, students should be critically aware of the content they access on-line and be guided to validate the accuracy of information.

Equally, students should be reminded to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

6.1.6 Students should be helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside SML College.

6.1.7 Rules for use of ICT systems will be posted in all rooms and may be displayed on log-on screens or desktop backgrounds.

6.1.8 Stakeholders should act as good role models in their use of ICT, the Internet and mobile devices.

6.2 E-safety education for parents/carers

6.2.1 It is widely accepted that some parents and carers have only a limited understanding of e-safety risks and issues and their own legal liabilities, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

6.2.2 The value of the termly meeting with parents/carers is it gives opportunity for the Learning Group Adviser to raise issues if it is apparent that usage outside SMLC is a problem. However serious concerns will be raised immediately with parents if needed.

6.3 We will advise that Stakeholders pursue E-safety education

6.3.1 It is essential that all Stakeholders understand their responsibilities, as outlined in this policy.

• All new Stakeholders should receive briefing on e-safety, ensuring that they fully understand the college E-safety policy and Acceptable Use Policies

• The E-Safety DSL will receive regular updates This will happen though training sessions/attendance at Local Authority /other information, and reviewing guidance documents released.

• The E-Safety DSL will provide advice/guidance as required to individuals as required

• The E-safety DSL ensures that all Stakeholders are aware of the procedures that need to be followed in the event of an e-safety incident taking place

6.3.2 This E-safety policy and any updates will be presented to and discussed with Stakeholders in monthly meetings

6.3.3 The E-safety DSL will provide advice/ guidance and will signpost training to Stakeholders where needed. As hired contractors, it is their responsibility to ensure that they are aware of e-safety issues and if they use online resources, that they are safe for students to access them.

6.4 E-safety for Trustees and Governors

6.4.1 The Trustees and Governors take seriously their responsibility to safeguard and promote the welfare of students. They appoint the E-safety DSL and ensure they have the status and authority within the management structure to carry out the duties.

7. The use of images of students

7.1 The development of digital imaging technologies has created significant benefits. Stakeholders and students can have instant use of images that they have recorded themselves or downloaded from the Internet. However, they need to be aware of the risks associated with sharing images and with posting digital images on the Internet.

Those images may remain available online and may cause harm or embarrassment to individuals, SML College will aim to inform and educate users about these risks and will act to reduce the likelihood of the potential for harm.

7.2 When creating digital images, Stakeholders need to re-enforce students' understanding of the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet.

7.3 Stakeholders are allowed to take digital/video images to support internal educational use only. Such images should only be recorded using SML College equipment; personal equipment belonging to Stakeholders should not be used for such purposes,

7.4 Care should be taken when taking digital/ video images that students are appropriately dressed and are not participating in activities that might bring the individuals or SML College into disrepute,

7.5 Students must not take, use, share, publish or distribute images of others without their permission,

7.6 Photographs published on the SML College website or elsewhere that include students will be selected carefully by the DSL, who will ensure that the appropriate checks and permissions will be sought prior to publishing,

7.7 Students' full names will not be used anywhere on the public website. This is to prevent third parties from identifying that a particular individual that attends SML College. Forenames can be used, e.g. "Sam".

7.8 Appropriate permission from parents or carers will be obtained before photographs of students are published on the SML College website or on the associated social media pages. This is part of the Acceptable Use Policy signed by parents/ carers on admission of their child. A list of those students whose image should not be used will be maintained by the DSL.

8. Technical e-safety provisions

8.1 SML College, in conjunction with the contracted ICT Services, will be responsible for ensuring that their infrastructure/ network is as safe and secure as is reasonably possible and that procedures set out within this policy are implemented:

8.2 The DSL will ensure that there are regular reviews and audits of the safety and security of ICT systems, alongside the contracted ICT Services that SML College use.

8.3 All Stakeholders will have clearly defined access rights to the ICT systems of SML College.

8.4 Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details. If there is a breach of security, this must immediately be reported to the DSL.

8.5 The administrator passwords for the ICT systems used and the ICT accounts must be available to the DSL. These passwords much be kept in a secure, physical or electronic location software with encrypted storage.

8.6 SML College, will use a sufficient Internet filtering system to restrict access to certain materials, adhering to current government guidelines and recommendations,

8.7 SML College will reserve the right to use internal monitoring systems to intercept and record any IT use for safeguarding and security purposes,

9. Responding to e-safety incidents

9.1 SML College will ensure that there are effective child protection mechanisms in place for students and Stakeholders to report any concerns that may arise. Any concerns should be reported to the DSL.

9.2 The E-safety DSL should;

- Liaise with ICT services, trustees and the Chair of Governors as necessary to investigate the alleged incident and establish evidence of any breach or wrongdoing,

- Work with any students involved to resolve issues and educate users as necessary,

- Inform parents/ carers of the incident and any outcomes,

- Where the alleged incident involves Stakeholders misuse, this will lead to an internal investigation

- Outcomes of investigations will be decided by the DSL and the Chair of Governors. This may lead to the contractual agreement to be ceased with immediate effect. If required, external services such as Social Services, Police Service and the Online Protection Service will be contacted.

10. Digital communications with students

SML College recognise the benefits of facilitating digital communications with students, whether it be e-mail or via any provided system. However, Stakeholders must be aware of the professional risks and potential for false or otherwise accusation of misconduct and / or unprofessional conduct.

11. Breaches of policy

Any violation of the standards, procedures or guidelines set out in this policy may be treated as a formal disciplinary matter, which could result in dismissal, legal prosecution or both.

12. Legal frameworks

It is the users' responsibility to ensure they are compliant and work within all UK and E.U. applicable legislation in regard to the safe and legal use of ICT at SML College.

This includes but is not limited to the following:

- The Sexual Offences Act 2003

- The Racial and Religious Hatred Act 2006

- The Computer Misuse Act 1990 (sections 1 – 3).

- The Police and Justice Act 2006

- Communications Act 2003

- Data Protection Act 1998

- Malicious Communications Act 1988

- Copyright, Design and Patents Act 1988

- Public Order Act 1986

- Protection of Children Act 1978

- Obscene Publications Act 1959 and 1964

- Protection from Harassment Act 1997.

- The Regulation of Investigatory Powers Act 2000 (RIP)

- The Telecommunications (Lawful Business Practice) (Interception of Communications)

Regulations 2000