



SYON MANOR
COLLEGE

E-Safety Policy



CONTENTS

1.0 Statement Page 3

2.0 Aims Page 3

3.0 Policy Scope Page 3

4.0 Definitions Page 4

5.0 Key People Page 5

6.0 Education and Training Page 5

7.0 Incidents and Reports Page 5

8.0 Appendices Page 6

1.0 STATEMENT

At Syon Manor College (SMC) we recognise the benefits and opportunities technology today has to offer different teaching and learning environments. We provide internet access to all students and staff through the use of on-site computers and personal work laptops. We encourage the use of these technologies to enhance skills, promote achievement and enable lifelong learning.

The internet and other information and communications technology provide great opportunities for learning and personal growth. However, they also present new challenges and can pose serious risks – such as sexual exploitation, grooming, sexting, cyberbullying, radicalisation and intrusion of data privacy. These occurrences can have profound and lasting effects on personal safety, mental and physical wellbeing, and the development of healthy relationships. SMC therefore makes all efforts, including technical and educational, to help create a safe yet flexible environment for using such technology at the College.

SMC maintains a zero-tolerance approach to any forms of abuse including bullying, whether online and/or in person, sexual harassment and violence, racist, sexist and homophobic (or any other transrelated phobias) behaviour and abuse. Students and staff are encouraged to report any concerns or issues, however small, to a trusted member of staff and/or the Designated Safeguarding

Document Type	Policy	Version Number	1.1
Policy Owner	Syon Manor College	Last Review Date	December 2023
Date First Issued	November 2022	Next Review Date	At least annually



Lead (DSL) so that appropriate and timely action can be taken, and relevant support offered. The DSL will always be informed of concerns raised.

2.0 AIMS

The aim of this policy is to demonstrate our commitment to the online safety of our students and staff. At SMC, we aim to:

- Identify responsibilities relating to e-safety at SMC.
- Encourage students to make good use of the educational opportunities presented by safely accessing the internet and other electronic communication.
- Safeguard and promote the welfare of students by preventing cyberbullying and other forms of abuse.
- Help students and staff take responsibility for their own e-safety.
- Ensure students and staff use technology safely and securely.
- Educate members of the SMC community about potential threats and harms arising from internet use.

3.0 POLICY SCOPE

This policy considers guidance issued by the Department for Education and should be read in conjunction with the college's Safeguarding Policy. This policy is to be used as a guide to all staff at SMC. It considers guidance issued by the Department for Education and should be read and understood alongside our other relevant school policies:

- SMC Social Media Policy
- SMC Web Filtering and Monitoring Policy
- SMC Safeguarding Policy
- SMC Health and Safety Policy
- SMC Mental Health and Wellbeing Policy
- SMC Positive Behaviour Management Policy
- SMC Equal Opportunities and Diversity Policy

4.0 DEFINITIONS

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.

5.0 KEY PEOPLE

All staff members have a responsibility to promote e-safety in the students' lives in and outside of college. However, certain staff members have a specific role in the process. These are:

- Assistant Head of Pastoral and Designated Safeguarding Lead (DSL): Ciaran Mckeever
- Principal and Deputy Designated Safeguarding Lead (DDSL): Carole Nicolson
- Assistant Head of Curriculum and Deputy Designated Safeguarding Lead (DDSL): Matt Ayling
- Safeguarding Governor: Ciaran Walsh

If a member of staff is concerned about a student's e-safety student, then in the first instance they should speak to the college DSL, Ciaran Mckeever.

6.0 EDUCATION AND TRAINING



With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and students. It is therefore our view, that the College 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

E-safety will be covered regularly in PSHE lessons. During this course of study students will have access to e-safety modules and tutorial sessions. During these sessions students are taught 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.

For Staff

Staff will take part in mandatory Safeguarding training (which includes e-safety) at least once a year. Further resources of useful guidance and information will be issued to all staff following the session. Staff attendance is recorded and monitored by HR.

7.0 INCIDENTS AND REPORTS

Where an e-safety incident is reported within the College this matter will be dealt with very seriously. SMC 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 any member of staff, their tutor, DSL or DDSL. Where a member of staff wishes to report an incident, they must contact the DSL as soon as possible. In any instance, the DSL must be informed and the incident recorded on Sleuth, the college's electronic safeguarding system. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Measures and consequences may be put in place in line with the College's Positive Behaviour Policy, 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 the Senior Leadership Team, in consultation with appropriate external agencies.

8.0 APPENDICIES

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 talk to your parents or carers before you go ahead with this and take a trusted adult friend along with you.
- Students or staff should report any abusive behaviour immediately to the DSL, Ciaran Mckeever.

Appendix B – Guidelines for Students (Social Media)

As part of our duty of care to our students, the college sets out guidelines, below, for students when using social media. These guidelines are made available to students in PSHE, the guidelines are also featured here to make staff aware of them. Students should follow the guidelines below at all times:

- Do not enter 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 college 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 incites 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 a college or course activity is optional. Students may opt out at any time.
- 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 our Anti-Bullying Policy.
- Students should report any abusive behaviour immediately to the DSL, Ciaran Mckeever.

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 **MUST** 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 college.
- 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 distracting.
- 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 DSL. Examples may include: student inappropriately dressed or in an inappropriate location (eg 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.
- 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 SMC 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 distracting.
- Eat or drink, other than water / tea / coffee
- Leave multiple applications open during the call as it may affect the quality.

The College has a clear policy on the use of mobile and smart technology which must be followed (Safeguarding policy)