



SYON MANOR
COLLEGE

Staying Safe Online Policy

Contents

1.0 PURPOSE	3
3.0 LEGISLATION AND POLICY FRAMEWORK.....	4
4.0 SUPPORTING STUDENTS AND YOUNG PEOPLE	5
5.0 EDUCATION AND TRAINING	5
6.0 UNDERSTANDING THE RISKS.....	7
7.0 HOW TO KEEP STUDENTS SAFE.....	11
8.0 RESPONDING AND REPORTING	13
9.0 STUDENT GUIDANCE	15
10.0 RESOURCES.....	16
11.0 APPENDICES	18

1.0 PURPOSE

At Syon Manor College (SMC), we are committed to ensuring that all students are always safeguarded, both offline and online. Their safety is our highest priority and must remain central to everything we do.

We recognise the benefits and opportunities that technology provides for teaching, learning and personal development. However, we also acknowledge the risks associated with its use. This policy sets out our approach to online safety and provides detailed guidance to help keep students safe when using digital devices, the internet and online platforms.

This policy applies to all students, staff, governors, volunteers and visitors and should be read alongside the college's safeguarding procedures.

2.0 POLICY STATEMENT

Technology is an integral part of everyday life and provides many opportunities for learning, communication and development. At SMC, we actively encourage the safe and responsible use of digital technologies to enhance learning, promote independence and support achievement.

However, technology also presents significant risks, including cyberbullying, exploitation, grooming, radicalisation, exposure to harmful content and online abuse. Students who are vulnerable offline may also be more vulnerable online. SMC maintains a zero-tolerance approach to all forms of abuse, including online abuse.

All staff have a responsibility to safeguard students and must act immediately on any concerns. Students are encouraged to report any concerns to a trusted adult so that appropriate and timely action can be taken.

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 staying safe online 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 online 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 LEGISLATION AND POLICY FRAMEWORK

This policy considers guidance issued by the Department for Education and this section outlines the legal and regulatory framework that underpins this policy, ensuring compliance with statutory requirements and promoting a consistent and effective approach to safeguarding across the college.

This policy is informed by current legislation, statutory guidance and Department for Education guidance, including:

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children 2026
- The Online Safety Act 2023 and relevant Ofcom guidance
- Department for Education guidance on filtering and monitoring in schools and colleges
- Department for Education digital and technology standards for schools and colleges
- Relevant data protection legislation and guidance
- Prevent duty guidance, where applicable
- Local safeguarding procedures and arrangements operated by the London Borough of Hounslow.

This policy will be reviewed at least annually and whenever there is a significant change to legislation, statutory guidance, local safeguarding arrangements, technology, or the online risks faced by students.

This policy should be read in conjunction with the following college policies:

- Safeguarding Policy
- Anti-Bullying Behaviour Policy
- Positive Behaviour Management Policy
- Social Media Policy
- Health and Safety Policy
- Mental Health and Wellbeing Policy
- Data Protection Policy
- Equality and Diversity Policy
- Web Filtering and Monitoring Policy
- Peer on Peer Abuse Policy
- Child and Young Person Exploitation Policy
- Anti Radicalisation Policy

The college operates appropriate filtering and monitoring systems to safeguard students when using college networks. These systems help to prevent access to harmful content; however, they cannot guarantee full protection, particularly when devices are used outside of the college network.

4.0 SUPPORTING STUDENTS AND YOUNG PEOPLE

SMC recognises that digital technology provides a wealth of learning opportunities. These opportunities must be balanced with appropriate safeguarding measures. Students are supported to:

- Recognise, understand and manage online risks
- Develop digital resilience and critical thinking skills
- Use technology safely, responsibly and respectfully

Online safety is embedded within the curriculum, particularly through PSHE, where students are taught about online risks, safe behaviours, and how to seek help. Students are encouraged to:

- Talk openly about their online experiences
- Report anything that causes concern
- Understand the importance of respectful online behaviour

Additional support and monitoring may be required for students with SEND, communication needs or vulnerabilities. This will be identified through individual risk assessments and planning.

5.0 EDUCATION AND TRAINING

Education and training are central to ensuring effective online safety. Due to the rapidly evolving nature of technology, risks cannot be completely eliminated; therefore, equipping students and staff with the knowledge, skills and confidence to respond appropriately is essential. A whole-college approach is taken to online safety education, ensuring consistent messages are delivered and reinforced across all areas of college life.

5.1 Student Education

Students receive structured and progressive online safety education through PSHE, mentor time and across the wider curriculum. This education is age-appropriate and adapted to meet the needs of different learners. Students are taught to:

- Understand the different types of online risks (content, contact, conduct and commerce)
- Recognise unsafe situations and early warning signs
- Develop critical thinking skills when engaging with online content
- Evaluate the reliability and accuracy of information

- Understand the impact of their online behaviour on themselves and others
- Know how and where to report concerns confidently

Opportunities are also provided for discussion, reflection and scenario-based learning to help students apply their knowledge in real-life situations.

5.2 Staff Training

All staff receive annual safeguarding training, which includes online safety. This ensures staff are equipped to identify risks, respond appropriately and support students effectively. Staff training includes:

- Awareness of current and emerging online risks
- Understanding safeguarding procedures and reporting expectations
- Recognising signs of online harm or exploitation
- Promoting safe and responsible technology use

Staff are expected to remain vigilant and proactive in identifying concerns.

5.3 Ongoing Professional Development

Online safety training is not limited to annual sessions. Staff receive regular updates, briefings and guidance throughout the year to reflect emerging risks, new technologies and safeguarding priorities.

Where appropriate, additional targeted training may be provided for specific roles (e.g. DSL, pastoral staff, IT staff).

5.4 Parental Awareness and Engagement

Parents/carers play a key role in supporting online safety. The college will:

- Provide information and guidance on current online risks
- Share advice on safe use of devices and platforms at home
- Encourage the use of parental controls and monitoring tools
- Promote open communication between parents/carers and children

Workshops, communications and resources may be used to support parents/carers in keeping young people safe online.

5.5 Monitoring and Evaluation

The effectiveness of online safety education is monitored through:

- Student feedback and discussions
- Staff observations
- Safeguarding records and trends

This ensures that education remains relevant, effective and responsive to emerging risks. The College will undertake an annual review of its online safety arrangements, supported by safeguarding reviews, monitoring processes and risk assessment activities, to ensure that online safety provision remains effective and responsive to emerging technologies and risks. Additional guidance and updates are provided throughout the year.

6.0 UNDERSTANDING THE RISKS

Online risks are constantly evolving, and it is essential that both staff and students remain aware of the different ways in which harm can occur. Understanding these risks enables early identification, prevention and appropriate response. Online risks can be categorised as:

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.

Conduct:

- Cyberbullying, harassment or abusive behaviour towards others online.
- Sharing, creating or distributing inappropriate, harmful or illegal content.
- Impersonation of others or the use of fake identities to deceive, manipulate or cause harm.
- Risky online behaviour, including sharing personal information or images that may compromise privacy or safety.

- Participation in online challenges, trends or activities that may result in physical, emotional or reputational harm.

Commerce:

- Exposure of minors to inappropriate commercial advertising.
- Exposure to online gambling services.
- Commercial and financial scams.

6.1 Harmful Content and Online Environments

Students may be exposed to harmful or distressing content online, either intentionally or accidentally. This may include:

- Pornographic or sexually explicit material
- Content promoting self-harm or suicide
- Racist, extremist or radicalising material
- Misinformation, fake news and conspiracy theories

Some online groups or forums may encourage harmful behaviours such as eating disorders, substance misuse or violence. Students should also be aware of the risks associated with harmful online challenges, trends and hoaxes that may encourage unsafe, dangerous or illegal behaviour. These can spread rapidly through social media platforms and may appear harmless despite presenting significant risks. It is important that staff remain aware of the content students are accessing and discussing. The 'dark web' is an area of the internet that is more difficult to access and may be used for illegal activities such as trafficking, illegal goods or accessing harmful content.

6.2 Cyberbullying

Cyberbullying is the use of digital technologies to bully, harass or intimidate others. This can occur via:

- Social media platforms
- Messaging apps
- Gaming environments
- Email or text messages

Cyberbullying can be persistent and may continue outside of college hours, impacting a student's wellbeing and mental health.

6.3 Sharing Images and Personal Information

Students may not fully understand the permanence of sharing information online. Risks include:

- Loss of privacy

- Identity theft
- Location tracking
- Reputational damage

Sharing images, particularly inappropriate or sexual images ('sexting'), can lead to exploitation, coercion or legal consequences. Once shared, images can be difficult or impossible to remove. Students should also be aware of the risk of sextortion, where individuals use sexual images, videos or information to blackmail, threaten or coerce someone into providing money, additional images or complying with further demands. Sextortion can affect anyone and should be reported immediately to a trusted adult, the DSL or the police.

6.4 Grooming and Exploitation

Grooming occurs when an individual builds a relationship with a young person to gain trust for the purpose of exploitation, abuse or radicalisation. This can occur through social media, gaming platforms or messaging apps. Students may not recognise that they are being groomed, particularly where the individual appears trustworthy or similar in age. Grooming may also be linked to sextortion, where offenders exploit trust, relationships or shared images to manipulate and financially exploit individuals. Early reporting is essential to ensure appropriate safeguarding support and intervention.

6.5 Apps, Gaming and Online Interaction

Many apps and games include features such as messaging, live streaming and in-app purchases. Risks include:

- Contact with strangers
- Exposure to inappropriate content
- Financial exploitation
- Excessive use or addiction

Students should be supported to use these platforms safely and in moderation.

6.5a Apps, Gaming and Online Interaction

Many young adults use social networking platforms, messaging services and dating applications to form relationships and communicate with others. While these platforms may provide opportunities for social interaction, they can also present safeguarding risks.

Risks may include:

- Contact with individuals who misrepresent their identity or intentions
- Grooming, exploitation or coercive behaviour
- Pressure to share personal information, images or videos
- Sextortion and online blackmail
- Emotional manipulation and abusive relationships
- Risks associated with meeting online contacts in person

Examples of platforms may include dating applications such as Tinder, Bumble, Grindr and similar services. Students should exercise caution when communicating with individuals online and should seek advice from a trusted adult if they have concerns about online relationships or interactions.

6.6 Online Scams and Fraud

Students may be targeted by scams designed to obtain personal, financial or account information. Common examples include:

- Phishing: Fraudulent emails designed to trick users into revealing information or clicking malicious links.
- Smishing: Scam text messages requesting personal information or directing users to fraudulent websites.
- Vishing: Fraudulent phone calls seeking sensitive information or payment.

Students should be taught how to:

- Recognise suspicious messages, links, attachments and requests for personal information.
- Verify the identity of individuals or organisations before responding.
- Avoid sharing passwords, personal information or financial details online.
- Report suspected scams, fraud attempts or security incidents to a member of staff immediately.
- Delete or ignore suspicious communications and avoid clicking unknown links or downloading unexpected attachments.

The college will promote awareness of online scams through age-appropriate online safety education and encourage students to seek advice from staff if they are unsure about the legitimacy of any communication.

6.7 Misinformation and Disinformation

Online content is not always accurate or reliable. Students should be supported to critically evaluate information, recognise bias and understand the impact of false information.

6.8 Additional Vulnerabilities

Some students may be at increased risk online, including those with SEND, mental health needs or those who are looked after. These individuals may require additional supervision, support and tailored risk management strategies.

Students with SEND may experience particular challenges in recognising manipulation, scams, grooming, coercive behaviour or misleading online content. Some students may be more trusting of others online or find it more difficult to identify potential risks. As a result, additional teaching, monitoring and support may be required to help them navigate online environments safely and confidently.

6.9 Emerging Technologies

Emerging technologies such as artificial intelligence (AI) and generative AI tools may present new risks, including misinformation, manipulation of content and reduced ability to verify authenticity. Students should also be aware of the risks associated with deepfake technology, where images, videos or voice recordings can be digitally altered or generated to appear genuine. Deepfakes may be used to spread misinformation, facilitate bullying or harassment, damage reputations, commit fraud or support exploitation. Developing critical thinking skills and verifying information through trusted sources is therefore increasingly important. Students should be supported to use these technologies safely and critically. Students are supported to understand these risks and how to respond appropriately, including how to seek help when needed.

The College recognises that generative artificial intelligence may create additional online safety, safeguarding, privacy, cyber security and misinformation risks. Students and staff should not enter confidential, personal or safeguarding information into generative AI tools unless the use of the tool has been authorised and is compliant with the College's data protection requirements. AI-generated images, videos, audio and text may be misleading or harmful. Students should be encouraged to question the authenticity of online material and seek advice from a trusted adult where content causes concern.

The College will keep its approach to generative AI under review as technology, risks and national guidance develop.

7.0 HOW TO KEEP STUDENTS SAFE

Keeping students safe online requires a proactive, whole-college approach that combines supervision, education, clear expectations and strong partnerships with parents/carers.

7.1 Managing Access

Internet access is filtered and monitored in line with statutory guidance. Access levels may be adapted based on age, need and individual risk assessments. Use of college devices and networks is supervised by staff. Students should not attempt to bypass filtering or security systems; this will be treated as a serious breach of behaviour expectations.

7.2 Setting Boundaries and Expectations

Clear expectations are established and reinforced consistently:

- Use devices only for appropriate educational purposes unless otherwise permitted
- Always follow staff instructions when using technology
- Demonstrate respectful and responsible behaviour online
- Understand that online behaviour is subject to the same expectations as offline behaviour
- Misuse of technology will be addressed in line with the Behaviour Policy.

7.3 Professional Boundaries (Staff)

Staff must always maintain professional boundaries. Staff must not communicate with students via personal social media, personal email accounts or private messaging platforms. Any online communication with students must be through approved college systems. Staff must always model safe and responsible online behaviour.

7.4 Student Communication and Reporting Culture

Students are encouraged to speak openly about their online experiences. A culture of trust is promoted so that students feel safe reporting concerns. Students are reminded regularly who they can speak to (e.g. tutor, DSL, any trusted adult).

7.5 Security, Privacy and Digital Literacy

Students are explicitly taught how to:

- Protect personal information and digital identity
- Use strong passwords and multi-factor authentication where appropriate
- Apply and understand privacy settings on apps and platforms
- Recognise unsafe requests for information

7.6 Use of Personal Devices and Mobile Technology

Use of personal devices is managed in line with the colleges Acceptable Use Policy. Devices may be restricted, monitored or removed where misuse is identified. Students must not use personal devices to access inappropriate content or communicate in ways that place themselves or others at risk.

7.7 Filtering, Monitoring and Limitations

The College uses appropriate filtering and monitoring systems to provide a safe digital and online environment for students and staff. Filtering is used to reduce access to illegal, inappropriate and potentially harmful online content. Monitoring is used to identify activity that may indicate safeguarding, wellbeing, behavioural or security concerns. Filtering and monitoring systems do not provide complete protection and must not be relied upon as a substitute for effective supervision, education and safeguarding practice.

The College will:

- Maintain appropriate filtering and monitoring arrangements in line with current Department for Education guidance.
- Ensure that safeguarding concerns identified through filtering or monitoring are reviewed and escalated appropriately.
- Ensure relevant staff understand their responsibilities for responding to monitoring alerts and safeguarding concerns.

- Regularly review the effectiveness of filtering and monitoring arrangements.
 - Consider the particular needs and vulnerabilities of students with SEND when assessing online risks.
 - Ensure monitoring and filtering arrangements are operated lawfully, proportionately and transparently, in accordance with data protection requirements.
 - Review arrangements when significant changes are made to systems, technology or online risks.
- Further operational detail is contained within the College's Web Filtering and Monitoring Policy.

7.8 Parental Engagement

Parents/carers are encouraged to support safe technology use at home. Guidance may be provided on:

- Parental controls
- Screen time management
- Age-appropriate apps and platforms

The college will communicate key messages and concerns where appropriate.

8.0 RESPONDING AND REPORTING

Immediate, proportionate and consistent action is essential when safeguarding concerns arise. Where an online 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. Serious incidents will be dealt with by the Senior Leadership Team, in consultation with appropriate external agencies.

8.1 Key Safeguarding Roles

Designated Safeguarding Lead (DSL): Joshua Tuckey
Deputy Designated Safeguarding Lead (DDSL): Matt Ayling
Safeguarding Lead for Governors: Nicola Mullarkey

The DSL has overall responsibility for safeguarding, including online safety. All staff share responsibility for identifying and reporting concerns.

8.1a Local Safeguarding Contacts

Where an online safety concern indicates that a child or young person may be at risk of harm, staff must follow the College safeguarding procedures and inform the DSL without delay.

Where an external safeguarding referral is required, staff should follow the current London Borough of Hounslow safeguarding referral pathway.

For a child who has been harmed or is at immediate risk of harm:

- London Borough of Hounslow Children's Services: **020 8583 6600** – select **option 2**, then **option 3**
- Out of hours: **020 8583 2222**
- In an emergency or where there is immediate danger: **999**

Staff should use the current Hounslow safeguarding referral process and should not delay a referral where there is an immediate safeguarding concern.

Contact details and referral arrangements will be checked during the annual policy review and whenever Hounslow safeguarding arrangements change.

8.2 Recognising Concerns

Concerns may arise from:

- Student disclosure
- Observed behaviour or changes in presentation
- Online monitoring alerts
- Reports from peers or parents/carers

All concerns must be taken seriously, regardless of perceived severity.

8.3 Reporting Procedures

Students should:

- Report concerns to any member of staff or directly to the DSL

Staff must:

- Act immediately
- Report concerns to the DSL without delay
- Record all concerns accurately on Sleuth

Staff must not delay reporting or attempt to investigate beyond initial fact-finding.

8.4 Responding to Incidents

The college will take appropriate action depending on the nature of the concern.

This may include:

- Providing immediate reassurance and support to the student

- Assessing level of risk and urgency
- Securing and preserving evidence where appropriate
- Removing access to harmful content or devices if necessary

Where required:

- External agencies (e.g. police, social care, Prevent) will be contacted
- Parents/carers will be informed, unless doing so would place the child at further risk

8.5 Specific Incidents

Additional considerations may apply to:

- Cyberbullying (managed alongside Anti-Bullying Policy)
- Sharing of indecent images (managed in line with safeguarding guidance)
- Online exploitation or grooming (immediate safeguarding referral)
- Radicalisation concerns (Prevent duty procedures)

8.6 Follow-Up and Ongoing Support

Following any incident:

- Risk assessments will be reviewed and updated
- Behaviour support plans will be reviewed and updated
- Educational interventions will be provided where appropriate
- Outcomes and wellbeing will be monitored over time

All actions will be recorded and reviewed to ensure effective safeguarding practice.

9.0 STUDENT GUIDANCE

Students play a key role in keeping themselves and others safe online. Clear expectations are communicated regularly and reinforced through the curriculum and daily practice.

9.1 Safe Behaviour Online

Students are expected to:

- Keep personal information private
- Only communicate with people they know and trust
- Use respectful language and behaviour
- Think carefully before posting or sharing content
- Understand that online actions can have real-world consequences

9.2 Protecting Themselves

Students should:

- Use strong and secure passwords
- Log out of shared devices
- Avoid sharing images or information that could put them at risk
- Block and report users who make them feel uncomfortable

9.3 Reporting Concerns

Students must:

- Report anything that makes them feel unsafe, worried or uncomfortable
- Not attempt to deal with serious issues themselves
- Seek support from a trusted adult as soon as possible

9.4 Respecting Others

Students must not:

- Engage in cyberbullying or harassment
- Share images or information about others without consent
- Participate in harmful online behaviour or challenges

Before posting, commenting or sharing content online, students are encouraged to consider whether their actions are:

True
Helpful
Inspiring
Necessary
Kind

Using the THINK approach can help students make positive and responsible decisions online. Any inappropriate behaviour will be addressed in line with the Positive Behaviour Management Policy and Safeguarding policies.

10.0 RESOURCES

Access to high-quality, up-to-date resources supports effective online safety practice across the college community. These resources are used to inform teaching, support safeguarding decisions and provide guidance to students, staff and parents/carers.

10.1 External Organisations

The following organisations provide trusted guidance and support:

- NSPCC – Online Safety Guidance: Advice on keeping children safe online, including reporting concerns and accessing support services.
- Childnet: Educational resources, lesson plans and guidance tailored to different age groups.
- Internet Matters: Practical advice for parents/carers, including device controls and platform-specific guidance.
- UK Safer Internet Centre: National guidance, reporting tools and resources linked to Safer Internet Day and current risks.

10.2 Use of Resources in College

These resources are used to:

- Support PSHE and curriculum delivery
- Inform staff training and safeguarding updates
- Provide guidance materials for students and parents/carers
- Respond to emerging risks and national safeguarding priorities

Students, staff and parents/carers can access these resources:

- Via the college website or safeguarding pages
- Through communications such as letters or workshops
- By requesting guidance from the DSL or pastoral staff

10.4 Reporting Through External Platforms

Where appropriate, concerns may also be reported via external organisations alongside internal safeguarding procedures. These include:

- CEOP (Child Exploitation and Online Protection Command) for concerns relating to online exploitation and grooming.
- Internet Watch Foundation (IWF) for reporting online child sexual abuse material and harmful content.
- Action Fraud for reporting online fraud, scams and cybercrime.

Reporting externally does not replace the requirement to report concerns to the DSL and follow the College's safeguarding procedures. These resources form part of a wider safeguarding approach and support the development of safe, informed and responsible online behaviours.

10.5 External Support and Reporting Services

Students, parents/carers and staff may access advice, support or reporting services through the following organisations:

Organisation	Purpose
--------------	---------

CEOP (Child Exploitation and Online Protection)	Reporting concerns relating to online exploitation, grooming and sexual abuse
Hounslow Local Safeguarding Contacts	Safeguarding Children and Young People London Borough of Hounslow Children's Services: 020 8583 6600 – select option 2, then option 3 (Monday to Friday, 9am to 5pm) · Out of hours: 020 8583 2222 · Immediate danger or emergency: 999 Safeguarding Adults London Borough of Hounslow Adult Social Care / Safeguarding Adults: 020 8583 3100 (Monday to Thursday, 9am to 5pm; Friday, 9am to 4:45pm) · Adult safeguarding concerns can also be referred through the London Borough of Hounslow's professional referral process. · Out of hours: 020 8583 2222 · Immediate danger or emergency: 999
Childline	Confidential advice and support for children and young people
ThinkUKnow	Online safety education and guidance for students, parents/carers and professionals
Internet Matters	Advice and resources for parents/carers on online safety
Report Harmful Content	Reporting harmful online content and obtaining support
Internet Watch Foundation (IWF)	Reporting online child sexual abuse material
Action Fraud	Reporting cybercrime, online fraud and scams

11.0 APPENDICES

The following appendices provide additional guidance to support safe, responsible and appropriate online behaviour. These appendices should be read alongside the main policy, Safeguarding Policy, Anti-Bullying Behaviour Policy, Positive Behaviour Management Policy, Social Media Policy, Health and Safety Policy, Mental Health and Wellbeing Policy, Data Protection Policy, Equality and Diversity Policy, Web Filtering and Monitoring Policy, Peer on Peer Abuse Policy, Child and Young Person Exploitation Policy and Anti Radicalisation Policy.

Appendix A – Student Online Safety Guidelines

Students are expected to always follow these guidelines to help keep themselves and others safe online.

Personal Information and Privacy

Students should:

- Keep personal information private and avoid sharing phone numbers, addresses, passwords, financial information or photographs with people they do not know and trust.
- Use strong and unique passwords for all online accounts, using a combination of letters, numbers and symbols.
- Never share passwords with others.
- Use privacy settings appropriately and review them regularly.
- Remember to log out properly after using websites, applications or shared devices.

Safe Online Communication

Students should:

- Be cautious when communicating online, particularly with individuals they do not know personally.
- Use private messaging only with people they know and trust.
- Understand how to block, mute and report users who make them feel uncomfortable or unsafe.
- Save messages, screenshots or chat logs where appropriate if evidence is needed.

Images, Videos and Digital Content

Students should:

- Think carefully before posting, sharing or forwarding content online.
- Remember that content shared online may remain accessible even after deletion.
- Never share inappropriate, indecent or sexually explicit images of themselves or others.
- Keep appropriate clothing on when using webcams or participating in online learning activities.
- Understand that sharing images without consent may cause harm and could result in disciplinary action.

Meeting Individuals Known Only Online

Students should:

- Think very carefully before meeting someone face-to-face whom they only know online.
- Never attend such meetings alone.
- Always discuss any proposed meeting with parents/carers or another trusted adult beforehand.

Reporting Concerns

Students must immediately report:

- Cyberbullying
- Abusive behaviour

- Inappropriate content
- Suspicious online contact
- Requests for personal information
- Any activity that makes them feel uncomfortable, worried or unsafe

Concerns should be reported to the Designated Safeguarding Lead (DSL) or another trusted member of staff as soon as possible. Failure to follow these guidelines may result in sanctions in line with the Behaviour Policy.

Appendix B – Student Social Media Expectations

As part of our duty of care, the College provides the following expectations regarding social media use.

Students must:

- Use social media responsibly, respectfully and safely.
- Not enter online friendships or relationships with individuals they do not know personally.
- Set privacy settings appropriately and review them regularly.
- Consider the long-term impact of online activity on their reputation, wellbeing and future opportunities.
- Understand that online actions can have real-world consequences.

Students must not:

- Use social media to harass, threaten, intimidate, insult, discriminate against or bully others.
- Share images, videos or information about others without permission.
- Access, promote or participate in content that encourages hatred, extremism, radicalisation or unlawful activity.
- Engage in gambling, identity theft, fraud or any other unlawful behaviour.
- Participate in harmful online challenges or activities.

Misinformation and AI Content

Students should:

- Critically evaluate information before sharing it.
- Be aware that online information may be inaccurate, misleading or deliberately false.
- Understand that artificial intelligence (AI) can generate realistic but inaccurate content.
- Verify information through reliable sources wherever possible.

Reporting Concerns

Students should report:

- Cyberbullying

- Harassment
- Harmful content
- Fake accounts
- Suspicious online activity

Any inappropriate online behaviour may be addressed through the Positive Behaviour Management Policy, Anti-Bullying Policy and Safeguarding procedures. Copies of inappropriate posts may be shared with parents/carers and, where appropriate, external agencies.

Appendix C – Online Learning, Webinar and Video Conferencing Expectations

Online learning should provide a safe, respectful and productive learning environment. Students are expected to:

- Join sessions on time and be prepared to participate.
- Behave respectfully and appropriately throughout sessions.
- Always use suitable language.
- Dress appropriately for a learning environment.
- Follow staff instructions.
- Not record, photograph or share sessions without permission.
- Only post chat messages relevant to learning activities.

During Online Sessions

Students should:

- Attend from a desk or suitable learning environment where possible.
- Use the blur background feature if attending from a bedroom or personal space.
- Ensure they are appropriately dressed.
- Look at the screen and engage actively with learning.
- Mute microphones when not speaking.
- Check what is visible on camera before joining a session.
- Minimise distractions wherever possible.

Students should not:

- Conduct or attend a session where circumstances would be inappropriate for a face-to-face lesson.
- Use inappropriate language or behaviour.
- Distract others intentionally.
- Use online learning platforms for non-educational purposes during sessions.
- Record, distribute or share content without permission.

Staff will ensure that online learning environments are safe, monitored and appropriate.

Appendix D – Staff Online Conduct and Video Conferencing Guidance

Staff must maintain the highest standards of professional conduct when communicating online.

Professional Boundaries

Staff must:

- Always maintain professional boundaries.
- Use only approved College systems to communicate with students.
- Never communicate with students through personal social media accounts, personal email addresses or private messaging applications.
- Avoid sharing personal information with students.
- Model safe and responsible online behaviour.

One-to-One Online Sessions

Where one-to-one online sessions are necessary:

- Sessions with under-18s or vulnerable students must be agreed in advance.
- Sessions should only take place at agreed times.
- Staff must ensure safeguarding training is up to date.
- Any concerns arising during sessions must be reported immediately to a line manager and/or the DSL.

If a staff member feels uncomfortable during a session, the session should be ended immediately and concerns reported.

Video Conferencing Expectations

Staff should:

- Always conduct themselves professionally.
- Use appropriate environments and blur backgrounds where necessary.
- Ensure appropriate dress standards.
- Be punctual and courteous.
- Test equipment before meetings.
- Mute microphones when not speaking.
- Minimise background distractions.
- Remind students that sessions may be recorded for safeguarding purposes.

Staff should not:

- Conduct online meetings that would be inappropriate face-to-face.
- Multi-task during meetings.
- Engage in distracting behaviour.
- Leave unnecessary applications running where this affects quality.

Appendix E – Acceptable Use of Technology

All users of college technology are expected to use systems responsibly, safely and in accordance with college policies.

Users must:

- Use systems for appropriate educational and professional purposes.
- Follow College rules and staff instructions.
- Respect the privacy, dignity and rights of others.
- Protect passwords and account details.
- Report security concerns immediately.

Users must not:

- Attempt to bypass filtering or monitoring systems.
- Access inappropriate, harmful or unlawful content.
- Install unauthorised software.
- Misuse College devices, networks or accounts.
- Use technology in a way that places themselves or others at risk.

The College reserves the right to monitor the use of its systems in line with safeguarding, security and legal requirements. Misuse of technology may result in disciplinary action and, where appropriate, referral to external agencies.