

Moor House School & College

E-Safety Policy



This version dated:	Summer Term 2025
This policy is to be read by:	All staff
Status:	Draft/Approved by ECM/Approved by FGB
Lead manager:	Darren Heine
Responsible committee:	ECM
Next review date:	Summer Term 2026

1. Scope and Context

Moor House School & College recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the school and college community to understand both the benefits and the risks, and to equip students with the knowledge and skills to be able to use technology safely and responsibly.

The E-Safety Policy relates to other policies including those focused-on cyberbullying, anti-bullying, behaviour management and for child protection.

2. Reason for policy

It is essential that children are safeguarded from potentially harmful and inappropriate online material.

3. Aim of policy

To have a have robust E-Safety Policy that sets out how to safeguard against and respond to E-Safety incidents. These must be understood and followed by all staff, volunteers, children and visitors.

4. Objectives of policy

- To have appropriate/effective filtering and monitoring systems in place.
- To ensure students are not being exposed to illegal, inappropriate or harmful content.
- To prevent students from being subjected to harmful online interaction with other users.
- To improve personal online behavior, to decrease the likelihood of harm being caused.
- To prevent cyberbullying.
- To providing education and on-going training to students and staff on how to use the internet safely.

5. Policy Statement

The purpose of this policy statement

Moor House School & College works with children and families because we believe that being aware of and practising E-Safety is the only way to mitigate these risks. They will always be present, but teaching young people and adults how to manage harmful situations and content will ensure they are best-placed to benefit from their time online, free from harm.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- provide staff and volunteers with the overarching principles that guide our approach to E-Safety.
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Moor House School & College's activities.

We will seek to keep children and young people safe by:

- appointing a Designated Deputy Safeguard lead with a specialist in E-Safety;
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others;
- supporting and encouraging parents and carers to do what they can to keep their children safe online;
- developing an E-Safety agreement for use with young people and their parents or carers;
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person;
- reviewing and updating the security of our information systems regularly.
- ensuring that user names, logins, email accounts and passwords are used effectively;
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate;
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse);

- providing support and training for all staff on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation;
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account;
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

6. Review

Review to be completed annually by DSL with specialism in E-Safety.

Appendices		Page Number
Appendix 1	Roles & Responsibilities	4-7
Appendix 2	Teaching & Learning	8-9
Appendix 3	Managing Internet access	9-10
Appendix 4	Published content and the Moor House website	11
Appendix 5	Social networking	11
Appendix 6	Managing filtering and emerging technologies Mobile Phones (Residential time)	12
Appendix 7	Mobile phones and smart watches Artificial intelligence (AI)	13
Appendix 8	Protecting personal data Authorising internet access Assessing risks	13
Appendix 9	Cyberbullying	14
Appendix 10	Handling E-Safety complaints and concerns	14-15
Appendix 11	Inappropriate contacts and non-contact sexual abuse	15
Appendix 12	Online child sexual exploitation (CSE)	16
Appendix 13	Contact with violent extremists	16
Appendix 14	Websites advocating extreme or dangerous behaviours	16-17
Appendix 15	Staff and the E-Safety Policy	17
Appendix 16	Enlisting parents' support	17
Appendix 17	Other policies and documents linked to this E-Safety document	17
ROLE	RESPONSIBILITY	
Governors	<ul style="list-style-type: none"> • Approve the E-Safety Policy • Monitor the effectiveness of the E-Safety Policy and that the necessary safeguards are in place. • Governors to confirm that policy is implemented and • monitoring/supervision systems are in place to identify children, young people and staff accessing or trying to access harmful and inappropriate content online. 	

Head Teacher and Senior Leads	<ul style="list-style-type: none"> • Ensure that all staff receive suitable CPD to carry out their E-Safety roles including online risks of extremism and radicalisation • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive E-Safety curriculum in place which is accessible to all students • Ensure that there is a system in place for monitoring E-Safety • Follow correct procedure in the event of a serious E-Safety allegation being made against a member of staff or pupil • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review E-Safety with the school's technical support • Work with the Designated Safeguard Lead (DSL)/Deputy Designated Safeguard Leads (DDSLs) to ensure that the Remote/Online Learning strategy developed and implemented by the school meets safeguarding and E-Safety requirements
E-Safety Lead	<ul style="list-style-type: none"> • Work with the school and colleges DSL and PSHE/ICT/Therapy staff • Lead the establishment and review of E-Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to E-Safety • Provide and/or broker training and advice for staff • Subscribe to appropriate newsletters websites and share information when it is received • Meet with SMT and/or Safeguarding Governor to discuss incidents and developments termly • Regular E-Safety training. • Source external monitoring to support the organisation and provide information for Governors to confirm that the necessary safeguards are in place. This monitoring doesn't need to be annually. It can be every 2-3 years as technology changes.
Moor House School & College Staff in Supporting E-safety	<ul style="list-style-type: none"> • To ensure that all approaches and strategies utilised to educate students at Moor House School & College and develop their awareness of safe online practices will take into consideration their speech and language impairment. • All staff should receive appropriate safeguarding and child protection training (including E-Safety) at induction. The training should be regularly updated. In addition, all staff

	<p>should receive safeguarding and child protection (including E-Safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.</p> <ul style="list-style-type: none"> • Staff will guide students to online activities that will support the learning outcomes planned for the students' age and maturity. • The school and college's Internet access includes content filtering which assists in filtering out potentially inappropriate content and monitors usage to provide audit trails. • Students will be taught about acceptable internet use and given clear guidance. • Students will be educated in the safe and effective use of the internet for research purposes, including the skills of navigation, knowledge location, information finding, retrieval and evaluation. • Students will be made aware of the dangers of giving out personal or private information online. • Students will be taught to be critically aware of the reliability of materials they access/view online and be shown how to validate information before accepting its accuracy. • Students will be taught to acknowledge the source of information used and respect copyright when using material in their own work. • Students will be taught how to report inappropriate Internet content. • Staff may contact students to relay information via official school channels: school e-mail, using school telephones and the school post. College staff use school mobile phones to contact students during staff working hours. • Staff must always use school e-mail addresses for school-related activities. • Staff must not contact students for matters that are unrelated to school. • Communications between staff and students must not occur through social networking sites, online video or audio calls, personal e-mail addresses or exchange chat messages, unless with the express and specific documented consent from the Senior Management Team. Classroom practitioners wishing to use Social Media tools with students as part of the school curriculum should risk-assess the websites before use and check the site's terms and conditions to ensure the site is suitable.
--	--

	<ul style="list-style-type: none"> • Any e-safety incident that involves any student at Moor House School & College will be dealt with as a safeguarding issue following procedures outlined in the school's Safeguarding, including Child Protection Policy. • In addition, the school and college will ensure there are specifically trained staff across the departments to whom concerns can be raised with regard to e-safety. These staff members are trained by a special Police service known as the Child Exploitation Online Protection Service (CEOP). • The school and college will be sensitive to Internet related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.
PSHE/ICT/THERAPY STAFF	<ul style="list-style-type: none"> • Work with the E-Safety and Computing Leads to embed and monitor a progressive E-Safety curriculum which is accessible to all students, as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum
Students	<ul style="list-style-type: none"> • Respect and Care for Equipment: <ul style="list-style-type: none"> - Handle computers, peripherals, and accessories with care. - Report any malfunctions or damage to a teacher immediately. • Appropriate Use. <ul style="list-style-type: none"> - Use computers only for educational purposes as directed by the teacher. - Access only authorized software, applications, and websites. • Internet Safety: <ul style="list-style-type: none"> - Do not share personal information online. - Avoid engaging in online conversations with strangers. - Be aware of and avoid suspicious links or downloads. • Digital Citizenship: <ul style="list-style-type: none"> - Be respectful and courteous in all online communications. - Avoid cyberbullying, harassment, or inappropriate language. • Privacy and Security: <ul style="list-style-type: none"> - Keep passwords private and secure. - Log out of accounts when finished. - Do not attempt to access others' accounts or private information. • Academic Integrity: <ul style="list-style-type: none"> - Do not plagiarize or copy others' work. - Acknowledge sources and give credit for borrowed content. • Time Management: <ul style="list-style-type: none"> - Use computer time efficiently and according to the task at hand. - Avoid distractions such as social media, games, or unrelated browsing during class. • Follow Moor House School & College Policies:

	<ul style="list-style-type: none"> - Adhere to the school's acceptable use policy (AUP) for technology. - Comply with teacher instructions regarding computer use. • Software Use: <ul style="list-style-type: none"> - Use software and applications as intended. - Do not install, uninstall, or modify software without permission. • Safe Handling: <ul style="list-style-type: none"> - Keep food and drinks away from computers. - Ensure hands are clean before using the computer.
Use of partner college platforms	<ul style="list-style-type: none"> • Students are supported by staff and taught how to use the partner college platforms. MHC STA'S facilitate the safe use of these systems.
Parents and Guardians	<p>Parents and guardians should work in partnership with Moor House and its staff in relation to any issues pertinent to E-Safety in the spirit of collaboration and to best protect the wellbeing of the child.</p> <ul style="list-style-type: none"> • Where possible, parents and guardians should implement parental control systems to limit Internet access to safe content only. • Endorse (by signature) the student AUP. • Keep up to date with issues through newsletters and other opportunities • Inform teacher/headteacher of any E-Safety concerns
Technical Support Provider	<ul style="list-style-type: none"> • Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack • Ensure users may only access the school network using an approved password • Support the school to ensure that platforms selected by the school for Online/Remote learning meet safeguarding and E-Safety requirements • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with E-Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the E-Safety Lead for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities

TEACHING AND LEARNING

The internet is an essential element in 21st century life for education, business, and social interaction.

Moor House has a duty to provide students with quality internet access as part of their learning experience. However, the benefits of internet access are tempered by its inherent risks, and the school and college is of course aware that all of its members, whether staff, parents or students, rely increasingly heavily on the digital world. It is a valuable tool for teaching and research, but the rules to infringe abuse need to be stringent and frequently reviewed.

We believe all students and other members of the Moor House community have an entitlement to safe internet access at all times.

Key E-Safety messages:

Students need to be guided on:

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that they won't be blamed if they report any E-Safety incidents
- that cyberbullying cannot be tolerated
- the basic principles of how to behave on the internet.

Staff are aware that some children may be more vulnerable to risk from internet use, generally those children with a high level of computer skills but coupled with poor social skills. The internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use. E-Safety is taught as part of the PSHCE programme in an age-appropriate way.

This is addressed each year as students become more mature, and the nature of newer risks is Identified.

- Students are taught how to report unpleasant internet content e.g. Telling a trusted adult.
- The students will have to read through and sign the student acceptable use policy (AUP).
- The school and college internet is filtered by Sophos and monitored by Securus.
- Moor House seeks to ensure that the use of internet-derived materials by staff and by students complies with copyright law.

- Moor House has two trained CEOP Ambassadors, one of these is a DDSL, and has an account with the National college which is used to train staff on E-Safety.

MANAGING INTERNET ACCESS

INFORMATION SYSTEM SECURITY

All members of staff have their own personal username and password which should be kept private.

When a member of staff leaves Moor House their account is disabled. Computers lock after a short period of inactivity to prevent access from unwanted people.

Staff accessing school and college systems at home take responsibility for ensuring they are using a secure computer. The Authenticator App is used for offsite access as an additional layer of security.

Computers logged into school and college systems should not be left unattended and when staff have finished working, they must log out of all systems to prevent unwanted access. Staff are encouraged to use Guacamole on the school system to access files at home rather than carry data on memory sticks, which can get lost.

- Staff are expected to change their passwords on a 3-monthly basis.
- Moor House School & College ICT systems security is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with the internet provider

MOOR HOUSE SCHOOL & COLLEGE SYSTEMS

Moor House School & College recognises that it is expected to do all it reasonably can to limit children's exposure to the risks posed by the internet and ensure that the school and college maintains appropriate filters and monitoring systems to prevent children from accessing harmful or inappropriate material from the Moor House IT system.

- The Securus monitoring system is in place to identify students who may be trying to access harmful and inappropriate material online – Securus will alert DSL and DDSLs if any attempt to view concerning content has been made. Securus provide Moor House with monthly reports that are used to review our system.
- Moor House has two safeguarding governors who meet with DSL and DDSL to discuss and E-Safety concerns and the systems we implement.
- The filtering is based on a category system, and there are blocks on the categories that are deemed inappropriate for school and college use. In line with government advice and the Prevent Strategy, these blocks include categories regarding terrorist and extremist material.
- Securus is a cloud-based application that monitors classroom computers and students' teams chats. It logs activity such as keywords, visual threats, and

phrases. The software is also in line with Ofsted guidance and takes keyword libraries from leading charities such as the Internet Watch Foundation and the Counter-Terrorism Internet Referral Unit.

- Sophos is our web filter, which auto-categorises websites and blocks pages depending on the categorisation. Similar to Securus, it also reports certain keywords. This is tested termly using: <http://testfiltering.com/test/> to ensure it blocks Adult Content, Child Sex abuse and Terrorism Content efficiently.
- Libra ESVA is our email filter; it uses a combination of AI and keyword lists to ensure the Staff and students don't receive any illicit or dangerous emails.

All web traffic is logged and monitored. If the content is on the blocked list, an 'access denied' page is displayed. If something inappropriate is accessed on the school computers, it must be reported immediately by a member of staff to a DSL or DDSL. The Moor House system is protected by an anti-virus system which scans all files. Emails are scanned for spam and dangerous attachments. When emails are blocked, the recipient is sent a report of what is blocked, from which they can request IT to allow it through.

Email

When using email, students are taught:

- not to disclose personal contact details for themselves or others
- to tell their parent or carer immediately if they receive an offensive or distressing email
- not to use email to bully or harass others
- be wary of opening attachments where they are unsure of the content

- E-Safety posters are displayed in the IT rooms and the site safeguarding boards.
- Students and staff may only use approved email accounts on the school system.
- Students must immediately tell a teacher if they receive an offensive email.
- Students are advised not to reveal personal details about themselves or others in email
- communication or arrange to meet anyone without specific permission.
- Staff to student communication can take place via email or Microsoft Teams. Emails must take place via a school email address will be monitored. Microsoft Teams can be used for communication but must only be used during school hours.
- External incoming emails should be treated as suspicious, and attachments not opened unless the author is known.

PUBLISHED CONTENT AND THE MOOR HOUSE SCHOOL & COLLEGE WEBSITE

The contact details on the website are the school and college's address, email, and telephone number. Staff or students' personal contact information is not published.

SOCIAL NETWORKING

When using social networking sites, students are taught:

- not to give out personal details to anyone online that may help to identify or locate them or anyone else
- not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted
- how to set up security and privacy settings on sites to block unwanted communications or deny access to those unknown to them
- to behave responsibly whilst online and keep communications polite
- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken

When using chat rooms, students are taught:

- not to give out personal details to anyone online that may help to identify or locate them or anyone else
- to only use moderated chat rooms that require registration and are specifically for their age group
- not to arrange to meet anyone whom they have only met online
- to behave responsibly whilst online and keep communications polite
- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken that any bullying or harassment via chat rooms or instant messaging may have serious consequences

Moor House School & College will control access to social networking sites and consider how to educate students in their safe use e.g. use of passwords. This control may not mean blocking every site; it may mean monitoring and educating students in their use.

- Students are advised never to give out personal details of any kind which may identify them or their location.
- Students are advised not to place personal information or photos identifying their address or school logo on any social network space.
- Students and parents are advised that the use of social network spaces outside school and college brings a range of opportunities; however, it does present dangers for users.
- Students are advised to use nicknames and avatars when using social networking sites.

MANAGING FILTERING

If staff or students come across unsuitable online materials, the site must be reported to the DSL or a DDSL.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.

A log of any incidents is maintained to identify patterns and student behaviour.

MANAGING EMERGING TECHNOLOGIES

When using web cameras, students are taught:

- to use them only with people who are well known to them
- not to do anything that makes them feel uncomfortable or embarrassed
- to tell their parents or carers if anyone is trying to force them to do something they don't want to do.

- Emerging technologies will be examined for educational benefit and potential risks assessed.
- Mobile phones and associated cameras are not be used during the school day (8.30-3.50/4:50), and students are expected to switch off their phones during these hours and keep them secure in reception. College students are permitted to carry their phones and use them when necessary.
- It is recognised that such hand-held devices may well not have any form of internet filtering when not connected to the WIFI.
- The sending of abusive or inappropriate text messages is forbidden.
- Wherever possible, staff will use a school or college phone where contact with students is required.
- The appropriate use of laptops and alternative learning platforms is discussed as the technology and resources become available within the school.
- Staff use of mobile devices is restricted during the school day when they are around students, and reference is made to this in the Staff Code of Conduct and initial safeguarding training.

MOBILE PHONES (Residential time)

School residential students keep their personal mobile phones in their lockers or in their personal box in the house. Mobile phones are only allowed to be used at set times and must be put away 30 minutes before bedtime. Exceptions to this is listening to music and checking messages from home. School students are not allowed mobile phones in their bedroom overnight.

College residential students keep their personal mobile phones on their person. They must come off their devices 30 minutes before bedtime. College residential students who are 16 and 17 years old are not allowed their mobile phones in their bedroom overnight.

College residential students who are 18+ are allowed to keep their mobile phones on them overnight. *This is subject to students following appropriate phone use.*

MOBILE PHONES AND SMART WATCHES (School students)

We recognise that mobile phones/smart watches are part of everyday life for many students and that they can play an important role in helping students to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- Students are not permitted to have mobile phones at school unless they turned off and kept in reception.
- Smart watches are not permitted to in school, they may be valuable and could be lost or stolen, as well act as a distraction in class. Where a student is found to be in unauthorised possession of a mobile phone/smart watch, the phone/watch will be confiscated and be placed in reception.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Moor House School & College recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Moor House School & College will treat any use of AI to bully pupils very seriously, in line with our behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

PROTECTING PERSONAL DATA

Personal data is recorded, processed, transferred, and made available according to the Data Protection Act 1998.

AUTHORISING INTERNET ACCESS

All staff must read and sign the staff Acceptable Use of Technology Policy.

Moor House School & College maintains a current record of all staff and students who are granted access to ICT systems.

Students and staff apply for internet access individually by agreeing to comply with the Acceptable Use Policy when they log on to any school computer or device.

ASSESSING RISKS

Moor House School & College will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Moor House cannot accept liability for the material accessed, or any consequences of internet access.

Moor House monitors ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate and effective. Software is installed

on the school network which enables staff to monitor the computers being used in a classroom. Staff can view what each student is doing with the exception of passwords.

CYBERBULLYING

Cyberbullying is defined as the use of IT to deliberately hurt or upset someone. Unlike traditional physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyberbullying is extremely prevalent as children who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous. In extreme cases, cyberbullying could be a criminal offence.

Cyberbullying may take the form of:

- sending rude, abusive, or threatening messages via email, text or social media
- posting insulting, derogatory, or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making and sharing derogatory or embarrassing videos of someone via mobile phone or email

Most incidents of cyberbullying will not necessarily reach significant harm thresholds and will probably be best dealt with the behaviour policies and the co-operation of parents.

In terms of Cyberbullying, students are taught:

- not to disclose their password to anyone
- to only give out mobile phone numbers and email addresses to people they trust
- to only allow close friends whom they trust to have access to their social networking page
- not to respond to offensive messages
- to tell a responsible adult about any incidents immediately.

HANDLING E-SAFETY COMPLAINTS AND CONCERNS

Complaints:

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the DSL and Principal.
- Complaints of a child protection nature must be dealt with in accordance with Moor House child protection procedures.
- Students and parents are made aware of the complaint's procedure.
- Students and parents will be informed of consequences and sanctions for students misusing the internet and this will be in line with the Moor House Behaviour Policies.

Parents and carers are advised to be vigilant about possible cyberbullying and how to cut down on the risk of cyberbullying:

- Blocking any mobile numbers or social media accounts that are engaging in cyberbullying
- Internet service providers can trace messages being sent from a personal email account and can block further emails from the sender where bullying takes place in chat rooms, the child should leave the chat room immediately and seek advice from parents; bullying should be reported to any chat room moderator to take action
- Website providers can remove comments from social networking sites and blogs and in extreme cases, can block the bully's access to the site
- The child could change mobile phone numbers or email addresses
- The child should take a photo or screenshot of any abusive comments/messages posted on social media and report it to their tutor or a trusted adult.

INAPPROPRIATE CONTACTS AND NON-CONTACT SEXUAL ABUSE

Concerns may be raised about a child being at risk of sexual abuse as a consequence of their contact with an adult they have met over the internet. If reported to Moor House School & College, students and parents are advised on how to terminate the contact and change contact details where necessary to ensure no further contact. Parents are advised to be vigilant of their child's internet use and report any concerns or incidents.

Students may also be sexually abused online through video messaging on social media platforms. In these cases, perpetrators persuade the student concerned to carry out sexual acts while the perpetrator watches/records them. The perpetrators may be adults but may also be peers.

In the event of such an incident, the child should be taught how to report via CEOPS (<https://www.ceop.police.uk/Safety-Centre/Should-I-make-a-report-to-CEOP-YP/>) and parents should contact the police to report the incident.

Staff and parents should contact Children's Services for advice on making a referral where there are concerns that the child:

- is being groomed for sexual abuse
- is planning or has arranged to meet with someone they have met on-line
- has already been involved in making or viewing abusive images
- has been the victim of non-contact sexual abuse.

If staff or parents are aware that a student is about to meet an adult they have contacted on the internet, they should contact the police on 999 immediately.

ONLINE CHILD SEXUAL EXPLOITATION (CSE)

CSE describes situations where a young person takes part in sexual activity either under duress or in return for goods, food or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example often the perpetrator is much older than the child, who may not aware that they are being abused.

Staff should be aware that children can be sexually exploited online, for example posting explicit images of themselves in exchange for money or goods.

If staff are concerned that a child they work with is being sexually exploited online, they should inform the DSL immediately, who may make a multi-agency referral.

CONTACT WITH VIOLENT EXTREMISTS

Many extremist groups such as far right groups, animal rights activists and fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

The Channel project is part of the government's Prevent strategy to divert young people away from extremism, and staff have received training. Staff need to be aware of those students who might be targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it is against the school's rules to access such sites.

Moor House School & College ensures that adequate filtering is in place, and reviews the filtering process whenever there is any incident of a student accessing websites that advocate violent extremism.

The DSL and DDSLs record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the service and where relevant would contact the relevant agencies to report the situation.

If there is evidence that a young person is becoming deeply enmeshed in extremist narrative, staff would seek advice from Surrey's Youth Support Services on accessing programmes under the Channel project to prevent radicalisation. Either contact Surrey via the email address: counter.extremism@education.gsi.gov.uk or call 020 7340 7264.

WEBSITES ADVOCATING EXTREME OR DANGEROUS BEHAVIOURS

Some internet sites advocate dangerous activities such as self-harming, suicide, or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

The mental health wellbeing team offer drop in sessions and alongside the DSL/DDSLs can offers support and someone for the students to talk to.

Moor House School & College uses R;pple, an organisation dedicated to intercepting harmful content related to self-harm and suicide through innovative technology. They will divert students to self-help advice and websites.

Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help. Where staff are aware that a young person is accessing such websites and that this is putting them at risk of harm, they should consider making a referral to the relevant Children's Services (depending on which county the child lives in).

STAFF AND THE E-SAFETY POLICY

- All staff are given the Moor House School & College E-Safety Policy
- All staff will sign to acknowledge that they have read and understood the E-Safety Policy and agree to work within the agreed guidelines.
- Staff are made aware in the Staff Code of Conduct that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use are supervised by senior management and have clear procedures for reporting issues.

ENLISTING PARENTS' SUPPORT

Parents and carers have access to the E-Safety Policy on the school website.

Moor House School & College will ask all new parents to sign the parent/student agreement when their child joins, and every existing student will be expected to read through the agreement with their tutors and sign the Acceptable Use Policy.

Moor House offers parents the chance to receive relevant E-Safety guidance by means of ParentMail, parent workshops and the opportunity to join our National College account.

OTHER POLICIES AND DOCUMENTS LINKED TO THIS E-SAFETY DOCUMENT

[Anti-bullying](#)

[Complaints](#)

[Data Protection](#)

[Safeguarding and Child Protection Policy](#)

[Staff Code of Conduct](#)

[Whistleblowing](#)