Moor House School & College

E-Safety Policy
January 2022

This Policy Is To Be Read By:	All staff who use technology when working directly with students; and staff and volunteers who supervise students when they are using technology
Review cycle:	Annually
Next review date:	November 2022
Status:	Draft /Being reviews/sent to ECM/Approved by ECM
The person responsible for this policy is	DDSL E-Safety
The committee responsible for this policy is	Every Child Matters

Moor House School and College is committed to safeguarding and promoting the welfare of children and young people regardless of their age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation. It expects all staff and volunteers to share this commitment.'

Executive Summary

- E-safety refers to the safe use of information systems and electronic communications
- The school and college has the appropriate monitoring in place to review Internet access and usage
- Moor House is committed to providing education and on-going training to students and staff on how to use the Internet safely and to creating an environment that does not tolerate Cyber-Bullying
- The purpose of this policy is to ensure everyone at MHS&C knows how to use the Internet safely and how to report a breach in the policy
- It is the intention to provide age and competency level specific access to internet content using MHS&C technology
  The policy provides the framework for third party technology to be used at MHS&C

This policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE and other statutory documents. This policy is used in conjunction with other school policies and has been developed by a working group, including representatives from all groups within the school.

The Online Safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place

Introduction and Guiding Principles

E-safety refers to the safe use of information systems and electronic communications. E-safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- E-safety concerns the safeguarding of children and young people in the digital world.
- E-safety emphasises learning to understand and use new technologies in a positive way.
- E-safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online and when using electronic communication of any sort.
- E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

ROLE	RESPONSIBILITY
Governors	Approve the Online Safety Policy • Monitor the effectiveness of the Online Safety Policy • 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 • Source external monitoring to support the organisation and provide information for Governors to confirm that the necessary safeguards are in place.
Head Teacher and Senior Leads	• Ensure that all staff receive suitable CPD to carry out their Online 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 Online Safety curriculum in place which is accessible to all students • Ensure that there is a system in place for monitoring Online Safety • Follow correct procedure in the event of a serious Online 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 Online Safety with the school's technical support • Work with the Designated Safeguard Lead (DSL) / Deputy Designated

	Safeguard Lead's (DDSL's) to ensure that the Remote/Online Learning strategy developed and implemented by the school meets safeguarding and online safety requirements
Online Safety Lead	• Lead the Online Safety working group • Work with the school and colleges DSL and PSHE / ICT/ Therapy staff • Lead the establishment and review of Online Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to Online 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.
School & College Staff in Supporting E-safety	• 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. • 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. • 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). (See Appendix 1 for names of current staff). • The school & 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	• Work with the Online Safety and Computing Leads to embed and monitor a progressive Online 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	• Students must tell a member of staff immediately if they receive an offensive e-mail or other form of electronic communication that may give rise to safeguarding concerns (also refer to Equality and Diversity Policy and Safeguarding, including Child Protection Policy). • Students must not reveal personal details of themselves or others in e-mail communication or on social networks. • Students must never arrange to meet anyone they have met through the internet, without specific permission to do so from their parent or guardian. • Students must not attempt to contact staff outside of school, via social networking sites, online video or audio calls, personal e-mail addresses or exchange chat messages. School e-mail is the most appropriate form of electronic communication with staff. • Students must inform a member of staff if they receive any incoming e-mails from unknown sources, avoid replying to the sender or forwarding the content, and avoid opening the attachments as these may contain computer viruses. • Read, understand, sign and act in accordance with the student Acceptable Use Policy (AUP)
Use of partner college platforms	• 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	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 well-being of the child. • 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 Online Safety concerns
Technical Support Provider	• 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 online safety requirements • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with Online 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 Online 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

Education of students

'Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), but schools and colleges should recognise that a one size fits all approach may not be appropriate and a more personalised or contextualised approach for more vulnerable children e.g. victims of abuse and SEND, may be needed.

Keeping Children Safe 2021

A progressive planned Online Safety education programme (ICT, PSHCE, Social skills, Residential care) takes place in line with 'Teaching online safety in schools', through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Within this:

- Key Online Safety messages are reinforced through assemblies, Safer Internet Week (February) and throughout all teaching
- Students are taught to keep themselves safe online and to be responsible in their use of different technologies
- Students are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material

- In lessons where internet use is pre-planned and where it is reasonable, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches

- Students are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- The online safety lead maintains and passes on knowledge of current concerns to be included within learning experiences

- Students are provided with opportunities to influence the online safety curriculum

- Students will sign an AUP for their class [which might be agreed class rules] at the beginning of each school year, which will be shared with parents and carers

- Students are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying' and given opportunities to support each other

- Students are supported to protect and managing their online reputation (a key factor for preparation to adulthood)

- Students to be supported with the management of online relationships (such as being advised on how to recognise who is a friend/not accepting friend requests from strangers)

- Students are supported managing health and well-being (such as the importance of self-regulating technology use and teaching strategies to do this)

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this by:

• Providing clear AUP guidance which they are asked to sign with their children

• Providing regular newsletter items and appropriate support materials

• Raising awareness through activities planned by pupils and staff

• Providing and maintaining links to up to date information on the school website

Training of Staff and Governors

There is a planned programme of Online Safety training as part of the overarching safeguarding approach, in line with Keeping Children Safe 2021 for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

• All staff knowing the Designated Safeguarding Lead and the Online Safety Lead and their responsibilities

• An annual audit of the Online Safety training needs of all staff

• All new staff and governors receiving Online Safety training as part of their induction programme, NQTs will be supported to complete the UKCIS Online Safety Audit Tool.

- Providing information to supply and student teachers on the school's Online Safety procedures
- This Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings
- Staff and governors are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 4772

Management of online sexual abuse and harassment

Peer on Peer Abuse

All members of staff are made aware that children can abuse other children (often referred to as peer on peer abuse). Children are encouraged to talk to members of staff if they feel they are the victim or perpetrator, or if they are aware of peer on peer abuse. This abuse may include:

Cyberbullying / harassment

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

- Students and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by; telling a trusted adult, Childline App and phone number 0800 1111, POSH helpline 0344 381 4772.

- Students, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.

- All incidents of online bullying reported to the school will be recorded and action taken by the school / College.

- The school / College will follow procedures to investigate incidents or allegations of online bullying.

- The school / College will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

- Students, staff and parents and carers will be required to work with the school to support the approach to online bullying and the school's Online Safety ethos.

- Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in the schools Behaviour Policy or AUP and may include:

- The bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content

- Internet access being suspended at the school for a period of time.

- The parent and carers of students being informed

- The police being contacted if a criminal offence is suspected

Management of Cyber bullying Please refer to Anti-Bullying Policy.

Sexting

The school will follow advice on how to respond to any incident of sexting. We will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL) or DDSL. An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) or DDSL will record any incident of sexting and the actions taken in line with advice from the Local Authority.

Sexual Harassment, including Upskirting

All staff are made aware that sexual harassment can occur between two children of any age and sex and can include online harassment. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence and can include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation; coercion and threats
- upskirting

All staff are made aware of what upskirting is, and that it is illegal. Any incident of sexual harassment will be taken seriously and reported to the Designated Safeguarding Lead (DSL) or DDSL. The Designated Safeguarding Lead (DSL) or DDSL will record the incident(s) and the actions taken and will inform the police if necessary.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

Data Protection

The school's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The school / college will:

- At all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates

- Use personal data only on secure password protected computers and other devices

- Ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data

- Provide staff with secure equipment/services to store or transfer data eg remote access, One Drive, encryption and secure password protected devices

- Remove data in line with the school's Data Retention Policy

- Ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead and that relevant staff understand the full requirements of Data Protection Act 2018

- Complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

Use of digital images and sound

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school / College's learning platform and to provide information about the school / College on the website. The school / College will:

- Build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging students to seek permission from other students to take, use, share, publish or distribute images and sound

- Ensure verifiable permission from parents or carers is obtained before images, sound recordings or videos of students are electronically published on the school / College website, on social media or in the local press. The written consent, where students' images, video and sound are used for publicity purposes, is kept until the data is no longer in use

- When using digital images, staff educate students about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites

- Allow staff to take images, record video and sound to support educational and therapeutic aims, following the school / College policy regarding the sharing, distribution and publication of those. School / College equipment only is used. Personal equipment of staff is not allowed for this purpose

- Make sure that images, sound or videos that include students will be selected carefully with their knowledge, taking care when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school / College into disrepute

- Make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed

- Ensure that students' full names will not be used anywhere on the school / College website, school / College blogs or within school / College branded social media, particularly in association with photographs

- Not publish students' work without their permission and the permission of their parents or carers

- Only hold digital/video images on school / College approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the school / College Data Retention Policy

- in accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school College events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others.

- Make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people

<u>Online/Remote Learning opportunities e.g. Microsoft Teams, Google Classroom,</u>

Moor House School & College will:

- Develop a strategic approach to Blended Learning which enables online/remote learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school / College

- Provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given

- Make sure that access to platforms will be password protected and run with approval from the Senior Leadership Team

- Ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content. This includes chat functions between staff and students. Any impropriate use could result in disciplinary action.

- Discuss the use of online/remote learning as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice and , being careful about subjects discussed online

- Register concerns regarding student' inappropriate use (in or out of school / college) and liaise with their parents and carers

- Support staff to deal with the consequences of hurtful or defamatory posts about them online

Personal devices

- Inform staff that personal devices should only be used in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher

- Ensure that staff understand that the AUP will apply to the use of their own portable / wearable device for school purposes

- Inform staff and visitors that they are not allowed to use personal devices to take photographs or video in school / College for any purpose without the express permission of SLT

- Check any use of a personal device for an education purpose (where permission has been given) only uses the school / College's internet connection on the school site

- Remind all that personal devices should be pin code or fingerprint protected and not discoverable by third parties

- Advise staff not to use their personal mobile phone to contact pupils, parents and carers

- Provide a mobile phone for activities that require them

- Challenge staff and visitors when there is suspected misuse of mobile phones or devices

- When students are allowed personal devices in school / College, they are used within the school /College's behaviour policy / code of conduct, and students understand they can be asked to account for their use

- Use the right to collect and examine any student device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school / College internet connection

E-safety Management within the School and College Community

Information System Security

- The security of the school and college information systems will be reviewed regularly by the IT Manager. A report will be submitted on a termly basis to SMT and the Finance Committee regarding actions taken and any recommendations.

- Virus protection will be updated regularly.

- Personal data sent over the Internet will be encrypted or otherwise secured.
- Technology that is not under the jurisdiction of Moor House School and College may not access the network unless agreed by the Senior Management Team. Where staff require remote access to the network this can only be authorised by a member of SMT and set up by the Network Manager.

- Students are permitted to copy their personal work on to portable storage devices to enable work at home and to practise backing up their work. Within the school environment, this process is supervised by the ICT teacher. Students will be prevented from downloading software to school computers, via their user privileges status. Staff will determine whether a download request is deemed suitable and necessary. A request can then be made, via the member of staff, to the IT Helpdesk to be put into effect.

- College students are encouraged to copy their work to portable storage devices for use at partner colleges and at home. They are supported by staff where necessary but independence in this area is encouraged.

- Unapproved software will not be allowed in students' user areas or attached to e-mail.

- All users of the system must agree to the school's Acceptable Use Policy (AUP).

Management of E-mail

- Staff will use only official school provided e-mail accounts to communicate with students and parents/carers, as approved by the Senior Management Team.

- Staff should not use personal e-mail accounts during their school working hours, unless doing so during their allocated break times/off duty, when students are not present/in the vicinity.

- Access to external e-mail accounts will be blocked if used at inappropriate times and must not be used to contact parents or students.

- Students may use only official school and/or link college e-mail accounts provided whilst at school.

- Excessive social e-mail use can interfere with learning and may be restricted.

- The forwarding of chain messages is not permitted.

- Staff must immediately tell their Line Manager if they receive offensive e-mail.

Management of School Website Content

- The contact details on the website should be the school and college address, e-mail and telephone number. Staff or students' personal information will not be published.

- SMT will take overall editorial responsibility for the school website, to review content and ensure that it is accurate and appropriate.

- The school and college website will comply with the school and college's guidelines for publications including respect for intellectual property rights and copyright.

- Students' full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images of students are electronically published

- Where a student has, for example, won an external award and it may be appropriate to publish their name with a photograph either on the school website or on a different platform; consent will be explicitly sought from the parents or guardians and from a member of the senior management team.

- Students' work can only be published with their permission or that of their parents/carers.

Management of Social Networking and Personal Publishing

- The school will control access to social media and social networking sites through the school and College's filtering system and list of approved websites. However, College students have access to social networking sites as a privilege which may be withdrawn without notice if used inappropriately.

- Newsgroups will be blocked unless a specific use is approved.

- Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc. However, an email address may be provided if deemed appropriate by the ICT teacher for example to sign up for presentation software such as Prezi

- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location for example house number, street name or school.

- Classroom practitioners' official blogs, wikis etc. should be password protected and run from the school website or approved school communication channels.

- Staff wishing to use social media tools with students as part of the curriculum should risk assess the site before use and check the sites terms and conditions to ensure the site is suitable. Documented consent must be given by the Senior Management Team before use.

- Classroom practitioners should use official e-safe networking spaces available online. Specific zones can be set-up within these networking environments to restrict access to Moor House students and staff only. Staff must not run social network spaces for student use on a personal basis.

- Students should be advised on security and encouraged to set safe passwords, deny access to unknown individuals and instructed how to block unwanted communications, if or when the need arises. Students should be encouraged to communicate to known friends only and deny access to others.

- Students should be advised not to publish specific and detailed private thoughts.

Management of Content Filtering

- The School & College will define the requirements for access control strategy to suit the age and curriculum requirements of the students. The IT Manager will implement the approach agreed.
- All breaches of Content Filtering Policy will the reported to the H&S Committee for review.
- The IT Manager will ensure that regular checks are made to ensure that the filtering methods continue to be effective.
- Any online material that the school believes is illegal will be reported to appropriate agencies such as Surrey Police, the IWF (Internet Watch Foundation) or CEOP (Child Exploitation and Online Protection Centre)**.**
- The school and college's internet access will include filtering appropriate to the age and maturity of students.
- If students discover unsuitable sites, they must report these to a member of staff. Staff will note the URL (website address) and report it immediately to the IT Manager and carbon copy the e-mail to the e-safety Coordinator and Designated Safeguarding Lead.
- Staff can make a request to the IT Manager to unblock sites which they deem appropriate in their professional capacity for student or staff viewing.
- Student access levels will be reviewed as necessary, to reflect the age of the students, educational requirements and changes to the curriculum.

Management of Emerging Technologies

- Emerging technologies will be examined for educational benefit and discussed with the Deputy Head Teachers, before they are introduced for use in school.

- The school utilises wireless technology. A public wireless network is utilised in the college. Students are permitted access to this facility, but the password is confidential and only privileged to staff. (Refer to the use of wireless, infra-red and Bluetooth communication technologies in the AUP.

<u>Policy Decisions</u>

The School and College will:

- Maintain a current record of any person who is granted access to the school's electronic communications.

- All staff and governors must abide by the Acceptable Use of Technology and Networks Policy (AUP)while using any school and college ICT resource.

- Take all reasonable precautions to ensure that users access only appropriate material.

- Audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.

- The school and college recognises that withdrawal of computer and Internet facilities for a student could have a detrimental effect on that student's progress and coursework grades. However the school will withdraw access in cases where it is deemed necessary.

- Parents will be informed that students will be provided with filtered Internet access.

Management of E-Safety Complaints

- Complaints of Internet misuse will be dealt with under the school's Complaints Procedure. Any complaint about staff misuse must be referred to the Principal. Students and parents will be informed of the complaints procedure. Parents and students will need to work in partnership with staff and the school to resolve issues.

- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Education Safeguards Team to establish procedures for handling potentially illegal issues.

- Any issues (including sanctions) will be dealt with according to the Moor House's disciplinary and/ or child protection procedures.

- All members of the school and college community will be taught or trained about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community. This forms part of the initial child protection training.

The police will be informed where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation:

- Child sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Pornography, adult or mature content
- Promotion of any kind of discrimination, racial or religious hatred
- Personal gambling or betting
- Personal use of auction sites
- Any site engaging in or encouraging illegal activity including radicalisation and terrorism
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / College
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

Communicating this E-Safety Policy

- Staff will have training in e-safety to raise awareness of the importance of safe and responsible Internet use.

- E-safety rules will be taught to every student and will be posted in ICT areas.

- An e-safety module will be included in the PSHE and/or ICT programmes covering both safe school and home use (see PSHCE and ICT policies).

- All users will be informed that network and Internet use will be monitored.

- Safe and responsible use of the internet and technology will be reinforced across the curriculum.

- 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 that manage filtering systems or monitor ICT use will be supervised by a member of the Senior Management Team and have clear procedures for reporting issues.

- Parents have the opportunity to receive information and training opportunities about e-safety. The Moor House E-Safety policy will be made readily available to parents on the website and e-mails will be sent to parents each year referencing the policy. Parents/carers are invited to annual parent workshops in order to receive information on E-Safety.

Review

- This policy will be formally reviewed annually by a multidisciplinary team of staff to check that it continues to represent our aims and practices. This team will be led by the Assistant Head Teachers and the Head of Residential Care.

- All students will be asked, through the School Council or Moor House College Forum, about their views on the use of Internet in the school and their views on this policy so that they may suggest amendments or improvements. Parents will also be asked.

- Heads of Department will also monitor the success of this within their departments throughout the year and provide feedback to the Senior Management Team if they have concerns about consistency of application.

Addition to reflect a move to 'blended learning' during the COVID-19 Pandemic

During any lockdown, partial closure or period of self-isolation students will need to access work. The Government has requested that schools and colleges deliver on-line learning that is equivalent to a day of learning. Staff will deliver our curriculum using a combination of set work, instructional videos and live lessons via Microsoft Teams. Therapy sessions will be delivered 1:1 via Teams.

Safeguarding protocols have been written and shared with staff, parents and students. These list the requirements of each whilst highlighting that it is everyone's responsibility to ensure safety whilst working on-line. They are summarised here;

- Students, staff and parents will be appropriately dressed.
- Staff and students will ensure backgrounds are clear and free of distractions.
- Sessions will be recorded and deleted after 31 days.
- Parents or carers will have to be present for any 1:1 sessions with students under 18.
- Students will be muted during live-lessons unless asked to share.

Moor House School & College are following the relevant guidance and best practice;

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

https://www.ncsc.gov.uk/blog-post/helping-school-staff-to-work-safely-online

Please also see the Moor House School & College Safeguarding Policy

APPENDIX 1

This policy links with the following other policies, which should also be read:

- Acceptable Use of Technology and Networks Policy
- Anti-Bullying Policy
- Child Protection, including Safeguarding, Policy
- Complaints Policy
- Staff A to Z

Safeguarding Leads:
Barbara Martin
Jon Mansell
Madeleine Van Niekerk
Daniel Carroll
Susie Simpson
Stephanie Williams
Helen Middleton
Darren Heine (Online Safety Lead)

CEOP Ambassadors:
Matthew Crowhurst – Teacher
Darren Heine- Residential Care Worker

Data & IT Manager:
Abdus Khasru

Online Safety Group
Darren Heine
Liz Brewer
Karin Robbins
Natascha Fulford
Abdus Khasru
Matthew Crowhurst

Sources:
Child Exploitation Online
Protection Website
http://www.ceop.police.uk
KCSIE 2021
Professionals Online SafetyHelpline

Additional Contact on E-Safety Issues:

If you are a member of school staff

- Contact the Education Safeguarding Team if you require advice on any aspect of safeguarding arrangements or incidents in schools and learning.
- To make a referral to Surrey Children's Single Point of Access (C-SPA) 0300 470 9100 please contact them directly. In an emergency you should call 999.

APPENDIX 2

Cyberbullying; Advice for head teachers and school staff

Ref: DFE – 00652-2014

PDF 195kb 6 pages

APPENDIX 3

Advice for parents and carers on cyberbullying

Ref: DFE 00655 – 2014

PDF 185kb 7 pages