COOMBE WOOD SCHOOL

E-safety Policy

Policy Area

Non-Statutory Document

Author

Headteacher

Version

1.2

Last Updated

January 2022

Adopted by the Local Governing Body (LGB)

Spring 2nd half-term 2022

Next Review

Spring 2nd half-term 2023

a folio education trust school

Statement of intent

At Coombe Wood School, we understand that computer technology is an essential resource for supporting Learning and Teaching. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

This policy contains detailed information regarding the dos and don'ts of ICT usage at CWS.

However, as an over-arching message to all members of the CWS community, we believe that always displaying the CWS core values (teamwork, respect, enjoyment, discipline and sportsmanship) whilst online will provide a very good starting point for appropriate, productive and safe ICT usage.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect students and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

Legal framework

This policy has due regard to all relevant legislation including,

but not limited to:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy will be used in conjunction with the following school policies and procedures:

- Child Protection Policy
- Anti-Bullying Policy
- Allegations Against Staff Policy
- Acceptable Use Agreement (staff and students)
- Behaviour Policy
- Data protection Policy
- Home School Agreement
- PSHE Policy
- Remote Learning Policy
- RSE and Health Education Policy
- Staff Code of Conduct

Use of the internet .

The school understands that using the internet is important when raising educational standards, promoting student achievement and enhancing teaching and learning.

Correct internet usage is in the statutory curriculum and is therefore an entitlement for all students, though there are a number of controls the school is required to implement to minimise harmful risks.

When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. content involving

radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Roles and responsibilities .

The Governing Body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.

The Headteacher, Ms N Williams, is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring online safety practices are audited and evaluated.
- Working with the DSL and Governing Body to update this policy on an annual basis.

The DSL, Mr T Clarke, is responsible for:

- Taking the lead responsibility for online safety in the school.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping students safe.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online

safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure (via CPOMS) for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the Governing Body about online safety on a termly basis.
- Working with the Headteacher and Governing Body to update this policy on an annual basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Students are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

E-safety education .

Educating students:

An e-safety programme is established and taught across the curriculum on a regular basis as a part of the PSHE curriculum, assemblies and tutor time activities, ensuring that students are aware of cyberbullying and the safe use of new technology both inside and outside of the school. Through PSHE and other relevant subject areas, students are taught:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or onlin coercion to perform sexual acts · Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate
- The CWS student diary (pages 24+25) contains information for students regarding where to access help and raise concerns.

Students learn about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.

Students learn to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.

All students sign the student acceptable usage agreement before joining the school. This agreement is embedded within the wider Home School Agreement that is freely available on the school website. From 2022-2023 onwards, a copy of this student acceptable usage agreement will also be added to the student diary for additional ease of reference.
Student pastoral voice highlights concerns around e-safety that are then managed

either by staff in school or by bringing in external agencies such as our Police Liaison Officers to further educate and support students to develop a positive and safe approach to online activities.

Educating staff:

All staff complete annual online e-safety training

All staff are aware of e-safety requirements and are up to date with any changes to the provision of e safety, as well as current developments in social media and the internet as a whole.

All staff employ methods of good practice and act as role models for students when using the internet and other digital devices.

The e-safety officer acts as the first point of contact for staff requiring e-safety advice.

Educating parents:

The school has received accreditation from, and continues to work with, National Online Safety to enhance the education offer to parents / carers relating to the online safety of their child.

Relevant E-safety information goes to parents through a variety of formats, including email, the school website and social media.

Parents / carer events (largely virtual) are offered to parents / carers on a regular basis by school comms.

E-safety control measures .

Internet access:

Internet access is authorised once parents and students have returned the signed consent form in line with our Acceptable Use Agreement.

Effective filtering systems are in place to eradicate any potential risks to students through access to, or trying to access harmful websites or use inappropriate material.

Filtering systems are used which are relevant to students' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

Any requests by staff to remove websites from the filtering list must be first authorised by the e-safety officer.

All school systems are protected by up-to-date virus software.

An agreed procedure will be in place for the provision of temporary users, e.g.

volunteers.

Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

Personal use will only be monitored by the e-safety officer for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.

Email:

Students and staff only use approved email accounts.

The use of personal email accounts to send and receive school data is prohibited. No sensitive personal data goes to any other students, staff or third parties via email.

Students are aware that all email messages are monitored and the filtering system will detect inappropriate links, viruses, malware and profanity.

Staff are not at fault when victims of cyber-attacks, as this may prevent similar reports in the future. The e-safety officer will conduct an investigation; however, this will only be to identify the cause of the attack, any compromised data and steps needed in the future to prevent similar attacks happening.

Social networking:

The school filters access to social networking sites as appropriate.

Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the e-safety officer.

Students are regularly educated on the implications of posting personal data online outside of the school.

Staff are educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

Staff must not communicate with students over social networking sites and should maintain their privacy settings.

Staff are not permitted to publish comments about the school which may affect its reputation.

Published content on the school website:

The Headteacher will be responsible for the overall content of the website and will

ensure the content is appropriate and accurate.

Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or students.

Images and full names of students, or any content that may easily identify a student, requires authorisation from parents.

Students must not take or publish photos of others without permission from the individual. Staff are able to take pictures, though they must not take pictures using their personal equipment.

Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:

Guidance regarding mobile phones and handheld devices is in the student diary and the staff hand book. It is also contained within the induction pack that all parents / carers receive before their child joins the school.

Network security:

There are network profiles for each student and staff member in which the individual must enter a username and personal password when accessing the ICT systems within the school.

Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.

Passwords require a mixture of letters, numbers and symbols to ensure they are secure as possible.

Students and staff set their own passwords on entry to the school to ensure maximum security for their school accounts. Breaches of password security are monitored and where necessary, regular password changes are introduced to increase security levels.

Passwords should be stored using non-reversible encryption.

Cyber bullying .

For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages or the posting of information or images online. Examples of this are not limited to, but could come

in the form of:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name • Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

The school recognises that both staff and students may experience cyber bullying and is committed to responding appropriately to instances that should occur.

We regularly educate students on the importance of staying safe online, as well as being considerate to what they post online.

Students are educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as the relationship and sex education curriculum.
At CWS, we commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.

We have zero tolerance for cyber bullying, and treat any incidents with the utmost seriousness in accordance with our Anti-Bullying Policy.

The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in the LA of the action taken against a student.

Peer-on-peer sexual abuse and harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The student believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The student does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The student may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the student feel 'special', particularly if the person they are talking to is older.
- The student may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. Staff annual online e-safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the

school and whom their close friends have not met.

- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain students at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a student relating to radicalisation, they will report this to the DSL without delay.

Mental Health

The internet, particularly social media, can be the root cause of a number of mental health issues in students, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a student's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a student is suffering from challenges in their mental health.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the student and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK

Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.

- Careful to avoid needlessly scaring or distressing students.
- Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger students but is almost exclusively being shared amongst older students.
- Proportional to the actual or perceived risk.
- Helpful to the students who are, or are perceived to be, at risk.
- Appropriate for the relevant students' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting students at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant students, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas
of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

Remote Learning

All remote learning is delivered in line with the school's Remote Learning Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents / carers prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents / carers to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents / carers to useful resources to help them keep their children safe online.

The school will support students through offering DFE provided technology and Data SIMS where possible, but will not be ultimately responsible for providing access to the internet off the school premises. The school will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Reporting misuse

Misuse by students:

Teachers along with the e-safety officer, have the power to discipline students who

engage in internet misbehaviour.

Any student who does not adhere to the rules outlined in our 'Acceptable Use Agreement' and is found to be wilfully misusing the internet may well have their internet use suspended.

Complaints of a child protection nature, such as accessing extremist material, receive action in accordance with our 'Child Protection Policy'.

The e-safety officer will consider whether the involvement of external agencies, including the Police, is appropriate and will act accordingly.

Misuse by staff:
Staff should report any misuse of the internet by a member of staff to the Headteacher immediately.

The Headteacher will deal with such incidents in accordance with the 'Allegations against Staff Policy', 'Code of Conduct Policy' plus any other related and relevant school policies which may lead the Headteacher to decide to take disciplinary action against the member of staff.

The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in the LA of the action taken against a member of staff.

Use of illegal material:

In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

If it is a child protection matter, the school follows the child protection policy, involving the DSL, Headteacher and the police.

Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.