COOMBE WOOD SCHOOL

E-safety Policy

Policy Area

Non-Statutory Document

Author

Headteacher / Designated Safeguarding Lead

Version

1.1

Last Updated

Spring 2nd half-term 2021

Adopted by the Local Advisory Board

Spring 2nd half-term 2021

Next Review

Spring 2nd half-term 2022

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.

Legal framework

This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation
- Freedom of Information Act 2000
- This policy also has regard to the following statutory guidance:
- DFE 'Keeping children safe in education'

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)
- Home School Agreement
- 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

It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

Folio Education Trust IT support, the Headteacher, the DSL and deputy DSL are responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard students.

The DSL (Mrs N Lattimore) acts as e-safety officer is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.

The Headteacher (Mr B Laker) is responsible for ensuring that the e-safety officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

The Headteacher and data protection officer (DPO – Mrs S Qureshi) will ensure termly GDPR walkabouts take place and are logged to monitor and support the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the Headteacher.

The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.

The local advisory board, Headteacher, e-safety officer and DPO will evaluate and review this E-safety Policy on a yearly basis, considering the latest developments in ICT and the feedback from staff/students.

All staff will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the HR Lead Officer for Folio Education Trust.

Parents are also responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

All students are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour and must read, understand and sign the student acceptable use policy before joining the school.

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, the safe use of new technology both inside and outside of the school. The CWS student diary (page 22) 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.

Clear guidance on the rules of internet usage are present in all classrooms containing ICT facilities.

Students know to report any suspicious use of the internet and digital devices to their classroom teacher.

Educating staff:

An online programme of e-safety training opportunities is available to all staff members, as outlined in the staff handbook.

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:

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

Parents' evenings, meetings and other similar occasions are utilised to inform parents of any e-safety related concerns.

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.

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.

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.

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'.

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' and may 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.