AEP

E-Safety Policy

Policy Owner **Sandeep Athwal**

AEP

Full Name	Position	Signature	Date	Review Cycle
Sandeep Athwal	Director		16.11.2023	Annual

Mission Statement

School of Coding is a safe, well ordered and caring environment for learning. It delivers high quality education to all its students and supports them to develop their individual potential for growth, self-worth and self-control.

High quality outstanding teaching, and clear and consistent guidance and support facilitates students in succeeding in education. Our broad and balanced academic and vocational curriculum will provide students with access to a broad range of accredited qualifications as well as educational and social experiences, which will address their learning and emotional needs. Our purpose is to support every student to develop their true potential, make positive contributions to their families and find fulfillment in employment.

Values

1. Alternative Provision doesn't mean a dumping ground…it's mainstream with the reasonable adjustments to succeed
2. High standards and high expectations are incredibly important and are the cornerstones to a successful school
3. School of Coding should become the go-to place for educators from across the country to see best practice
4. Good simply isn't good enough
5. Learning is about a journey and there is more than one way to get to the destination
6. Qualifications, manners, respect and opportunity should be the foundations for students that need a second chance.

School Ethos

High standards – students are pushed to achieve beyond their potential, and staff work to ensure everything that we do is better than people expect.

Daring to Dream – students at School of Coding may have been in an educational setting where they lacked aspiration to be successful, at School of Coding we challenge students to reach their potential and go on to further education and

AEP

employment.

Traditional Values – some things often get forgotten in education, at School of Coding we pride ourselves on mutual respect, good manners, making a positive contribution, supporting one another and an orderly, and litter free environment.

AEP

Success – can come in many virtues, at School of Coding we celebrate the small steps every day and tell students when they are doing well. We ensure that students can have a successful future.

Personalized Support - all students at School of Coding have a Learning Coach who guides them, sets them bespoke targets and supports them in making social and academic progress.

Statement of Purpose

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, children are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy, supported by the Acceptable Use Policies (AUP; see appendices) for staff, visitors and students, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: child protection, digital images, health and safety, behaviour and PSHE.

Both this policy and the Acceptable Use Policies (for all staff, visitors and students) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc.) and technologies owned by students or staff.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging

- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A comprehensive e-Safety education program for students, staff and parents.

Staff Responsibilities

E-Safety is recognized as an essential aspect of strategic leadership in this school and the Education Quality Manager aims to embed safe practices into the culture of the school. The Education Quality Manager ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture to address any e-safety issues which may arise in classrooms daily.

The responsibility for e-safety has been designated to a member of the senior leadership team.

School of Coding e-safety coordinator is Suki Gill (Education Quality Manager).

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with NSPCC and through organizations such as The Child Exploitation and Online Protection (CEOP) and 360 degree safe. The school's e-Safety Coordinators ensures the Senior Leadership Team are updated as necessary.

AEP

Sexting What is Sexting?

The term ‘Sexting’ means different things to different groups of people but Sexting is risky and is a Safeguarding concern. Sexting is the use of digital technology to record and send sexual photos, images, videos as well as text messages, with others online. Children are often unaware of the law, risks, dangers and consequences of Sexting. Sexting can happen between adults and children but also amongst children themselves.

Please refer to our Safeguarding Policy for further information.

Staff awareness

- All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.
- New staff receive information on the school’s AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-safety incidents are recorded on SIMS and to the DSL.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarized in the AUPs.

Internet:

- School of Coding will use Impero “filtered” Internet Service, which will minimise the chances of students encountering undesirable material.
- Staff, students and visitors have access to the internet through the school’s fixed and mobile internet technology.
- Staff should email school-related information using their @schoolofcoding.org address and not personal accounts.
- Staff will preview any websites before recommending to students.
- Search engines have ‘safe search’ activated by default.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- The CEOP Report Abuse button is available on the school website.
- Teachers make children aware of this and when it is appropriate to use it.
- If staff or students discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety coordinator(s) detailing the device and username.

- Staff and students are aware that school-based email and internet activity is monitored and can be explored further if required.
- Students using the World Wide Web are expected not to deliberately seek out offensive materials. Should any students encounter any such material accidentally, they are expected to report it immediately to a teacher who will contact IT Support and block further access to the site.
- Students are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.
- They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Students consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.
- The internet must not be used to search for or to spread material that could be considered to have extreme views against individuals, religion etc.
- A summary of these ICT rules are displayed in the ICT suite and all areas with ICT resources.

Keeping Children Safe in Education 2023 has outlined requirements for schools online safety policy and procedures as below. It is important that the online safety policy reflects procedures as set out for safety, behaviour and anti-bullying where child on child sexual abuse is a concern.

Online safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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

content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower-case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile technology (laptops, iPads, netbooks, etc.):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.
- Mobile technology for student use, such as iPads and netbooks, are stored in a locked cupboard.
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorized people cannot access the content.
- When they are not using a device, staff should ensure that it is locked to prevent unauthorized access.

Data storage:

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one or to the Office 365 Account/Dropbox.
- The school discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.
- Staff laptops should be encrypted if any data or passwords are stored on them.
- One Page Profiles, assessment records, student medical information and any other data related to students or staff should not be stored on personal memory sticks but stored on the school network.

- Only take offsite information you are authorized to and only when it is necessary and required to fulfill your role. If you are unsure speak to a member of the Senior Leadership Team.
- All personal information is accessible through secure online services removing the need to take information off site.

Social Networking Sites:

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school students or parents be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to School of Coding, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School Dismissal and Disciplinary Policies apply.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The school expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use. Any comments made by other members of staff that concern or worry you should reported to your line manager

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content.

The School reserves the right to monitor staff internet usage. The School considers

that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

AEP

Digital images

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children.
- Ensure you are aware of the children whose parents/guardians have not given permission for their child's image to be used in school. An up to date list is kept in the school administrative office.
- When using children's images for any school activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you. Providing a comprehensive E-safety education to students and parents.

All staff working with children must share a collective responsibility to provide e-safety education to students and to promote e-safety in their own actions.

Formally, an e-safety education is provided by the objectives contained in the Skills Sessions. Even if e-safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum. This is regularly reiterated via assemblies to all year groups.

Informally, a talking culture is encouraged in classrooms which allows e- safety issues to be addressed as and when they arise.

The e-safety coordinator will lead an assembly each year, highlighting relevant e-safety issues and promoting safe use of technologies.

Staff will ensure children know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the E- safety coordinator.
When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's ICT guidelines.

Parents/careers will be invited to attend an e-safety awareness workshop once per year.

Complaints procedure

As with other areas of school, if a member of staff, a child or a parent / career has a complaint or concern relating to e-safety then they will be considered, and prompt action will be taken. Complaints should be addressed to the e-safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern

will be recorded on SIMS and reported to the school's DSL. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Monitoring

Authorized members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorized use or suspected misuse of ICT must be immediately reported to the school's DSL or one of the e- Safety coordinators.

AEP

ICT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from e-safety incidents and promote a safe e-learning environment for students.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will not disclose my password to anybody else.
- When accessing school emails, Frog or any other sensitive information relating to School of Coding, employees will ensure that it is conducted on a device that had the appropriate security measures (anti-virus, firewall, encryption) and that locked out when away from the device and logged off each of the sites after use.
- I will ensure that any online communications with staff, parents and students are compatible with my professional role.
- I will not give out my own personal details to students or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of students will only be taken and used for professional purposes in line with school policy with consent of the parent or career. Images will not be distributed outside of school without the permission of the parent/career and Education Quality Manager.
- I will report any e-safety concerns to the designated safeguarding officer immediately.
- Mobile phones will be out of sight and switched to silent.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's e-safety policy and help students to be safe and responsible in their use of ICT and related technologies.

Signed:_____Print:_____Date: _____