The Study School
Internet and E-Safety Policy including EYFS

E SAFETY & INTERNET USE POLICY

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use, which may impact on social and emotional development and learning.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Zoom)
- Online chat rooms
- Online discussion forums
- Online games (e.g. Roblox, Minecraft etc)
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. YouTube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

This policy sets out how we strive to keep children safe with technology while they are in school and how they can apply this safety to their computer use at home. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the

school environment (parents, friends and the wider community) to be aware and to assist in this process.

Responsibilities: E-Safety coordinator

Our E-Safety officer is Mr McAuley. His role is to:
• Review and monitor this E-Safety policy.
• Consider any issues relating to school filtering
• Discuss any E-Safety issues that have arisen and how they should be dealt with.

Our E-Safety officer is the person responsible for the day to day issues relating to E- Safety. The E-Safety officer:
• takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents
• ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident
• ensures that e safety is embedded in computing lessons and children are aware
• provides training and advice for staff on a yearly basis
• provides training and advice for teachers on a yearly basis
• receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments
• has responsibility for ensuring the school's filtering system is working effectively
• maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

Responsibilities: head teacher

• The head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety is delegated to the E-Safety coordinator
• The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:
• they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
• they report any suspected misuse or problem to the E-Safety coordinator
• digital communications with students should be on a professional level and only carried out using official school systems
• E-Safety issues are embedded in the curriculum and other school activities.

General Use of School Computers

The use of school computers by pupils is permitted for purposes as directed by the school. The school has the right to look at any files on their systems including text, graphics and emails. Users are not permitted to access and amend another user's work without permission. Users must not give access passwords to other users. Using another user's password is not permitted.

All computers are protected by anti-virus software, which is kept up to date to check for the latest viruses. Any infections must be reported to the Computing coordinator, removed and the source (if known) notified.

No files should be brought into a school from home and loaded onto a school system without the permission of staff.

In cases where an individual has deliberately ignored school policy, the school reserves the right to deny access to school computer systems, including use of the Internet and email. This may have a negative impact on a pupil's education.

Hardware and software must be checked by the Computing coordinator before being installed on school computers.

Computer Equipment

All computer equipment must installed professionally and meets health and safety standards.

Projectors are maintained so that the quality of presentation remains high.

All computer equipment has anti-virus / spyware installed.

ICT systems must be reviewed regularly with regard to health and safety and security.

Internet Access

The school provides Internet and E mail access for educational purposes and should only be used by pupils and staff for these purposes.

The school uses Virgin Media who provide the school with a fibre optic Internet connection and the firewall and filter will be provided by Smoothwall. Pupils cannot use computers without filtered access. All Internet access by pupils is supervised by a member of staff or other responsible adult.

No pupil or member of staff is permitted to access material that is illegal, defamatory or potentially offensive using school systems. The copyright and intellectual property rights of material accessed using school systems must be respected.

Additionally the following activities are also considered unacceptable on ICT equipment / wi fi provided by the school:

- 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
- 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 (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

When children are admitted to The Study School, parents will be asked to sign a contract indicating they understand the issues and give consent for their child to use the Internet. This contract will also outline that pupils are not expected to actively attempt to access or distribute unacceptable material on school systems.

Use of school Wi-Fi only with permission of SMT and subject to the above conditions.

The Use of Email

Any user of the school email system must not use the system to communicate offensive, suggestive or defamatory material. It must not be used to harass another individual. Email messages sent and received from school systems should not be considered private. Pupils and staff should expect that emails could be inspected at any time.

Publishing on the Internet

The school has its own web site. Ultimate responsibility for content rests with the Head teacher.

The following guidelines will be followed:

- The school is appropriately registered under the Data Protection Act
- Individual pupils will not be identifiable by full name.
- Names will not be linked to pictures or individual email addresses.
- No personal information will be published without the individual's permission – this includes staff.
- Systems have been put in place to ensure that, where appropriate, information published is kept up to date.
- No copyright material will be published without the copyright owner's permission.
- Links will not be made to web sites which contain material deemed to be unsuitable.
- Access to web space will be restricted to ensure that only those with appropriate authority can publish to the school web site.

Parents are informed in general terms that this is happening and are asked to indicate that they are happy for their child to be included on the web site within the publishing guidelines that are sent to parents. Cases outside the scope of the guidelines are dealt with on an individual basis.

Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:
Members of staff are permitted to bring their personal mobile devices into school but these MUST be placed in the staffroom. Taking into of phones out of class/around school is a serious issue. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:

- Mobile phones will be used in the staff room only - in an emergency the school office can be contacted
- iPads used during teaching time for educational purposes only and must adhere to all other conditions in this document when doing so.
- Pupils who need personal hand held devices for after school hours must hand them into the school office at 8.30 am. They must not be used on site.

E-Safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:
• A planned e-safety programme is provided as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school – Go-Givers, Welcome to the Web, Think U Know sites.
• Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
• Pupils should be encouraged to adopt safe and responsible use of ICT both within and outside school.
• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils are allowed to freely search the internet, e.g. using search engines, ***staff should be vigilant in monitoring the content of the websites the young people visit***.

Posters are placed in each classroom to guide pupils to be
S Be **S**afe
M Don't **M**eet up
A **A**ccepting Emails can be dangerous
R **R**eliable?
T **T**ell someone

The Use of images

Images can be captured using an iPad or some of the applications on a laptop like Scratch, Windows Movie Maker. The images will be stored on the iPad device or the child's folder on their designated laptop (if they choose to save the document) which are then backed up onto the server.

Audit / Monitoring / Reporting / Review

All users have a responsibility to report immediately to class teachers / E-Safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

The E-Safety Officer will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

The E-Safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place.

Version control

Date of adoption of this policy	September 2020
Date of last review of this policy	January 2023
Date for next review of this policy	Spring 2025
Policy owner (SMT)	Head
Policy owner (Proprietor)	Amit Mehta