Stockport School

E-Safety Policy

This policy contains the following documents:-

E-Safety Policy

Pupil E-Safety and Acceptable Use Agreements

Parent / Carer Information Letter

Introduction

Computer based technologies has become an integral part of our everyday lives both in work and personal environments. As a professional educational institution, it is our responsibility to ensure our pupils have access to these technologies and use them to enrich their learning experiences. However, we have a responsibility under the Children Act 2004 to safeguard and promote the welfare of pupils. The strategies outlined in this policy enable the staff at Stockport School to create a safe e-learning environment that:

- Promotes the teaching of E-Safety across the curriculum not solely in computing lessons
- Protects children from harm
- Safeguards staff in their contact of pupils and their own use of the internet
- Ensures the school fulfils its duty of care to both staff and pupils
- Provides clear expectations for all on acceptable use of the internet

A broad definition of E-Safety:

An awareness of all fixed and mobile technologies that children and young people may encounter, now and in the future, which allows them access to content and communications that could raise issues or pose risks to their wellbeing and safety. As a professional educational institution, we will:

- Promote E-Safety across the curriculum
- Provide staff with up to date training
- Support the parents/guardians of our pupils
- Provide E-Safety resources for staff
- Ensure that schemes of work where ICT is used reflect this policy

E-Safety and acceptable use policy

1. Implementation and review

This policy relates to other policies including those for use of ICT, and for child protection.

The E-safety Policy outlined below applies to all pupils and parents at the school.

The school will identify a member of staff to co-ordinate e-safety. It has been determined that the school child protection officer and Adrian Didcote, Assistant Director of Computing will undertake this task.

This E-Safety Policy has been written in conjunction with current practices and builds on government guidance. It has been agreed by the Head teacher (Mr I Irwin) and the governing body.

The audience for this policy is parents, carers, teachers, school leaders, and network managers, and any other professionals concerned with child protection or use of digital facilities in schools.

The policy was revised by: Mr A Didcote (Assistant Director of Computing) and Mr J Warren (Designated Child Protection Officer and Senior Deputy Head teacher) in Oct 2020.

The policy and its implementation will be reviewed annually.

2. Teaching and learning –Pupils and the Web

Why internet use is important

The internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the curriculum and a necessary tool for staff and pupils.

'New technologies are integral to the lives of all children, young people and their parents. They inspire children to be creative, communicate and learn. It is essential that children and young people tap into the potential of the digital world if they are to enjoy their childhood and succeed in life. In educating children and young people, we should empower them to learn how to use digital technology responsibly not simply block what they can access. We must give them the information and skills they need to be digitally literate and savvy users. This enables them to take advantage of the opportunities that new technologies can offer, as well as being able to deal with any risks that arise'

Dr Tanya Byron

2.1 Internet use will enhance learning

Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2 Pupils will be taught how to evaluate Internet content and make decisions affecting their privacy

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught about privacy issues such as identity theft, fraud, and phishing. They will receive guidance about when to give out personal information (e.g. buying goods from secure websites) and precautions when creating 'posts' on public domains and social network areas.

2.3 Pupils will be taught how to identify potential risks associated with modern computer based technologies

Pupils will be taught how to identify potential risks to themselves and others such as exposure to inappropriate content, lifestyle websites, for example self-harm/suicide sites/hate sites.

2.4 Pupils will be taught about contact and conduct when using modern computer based technologies

Pupils will be taught about the potential dangers which revolve around contact and conduct with others on the web. This includes the potential for grooming, cyber-bullying, identity theft/privacy issues and disclosure, sexting, copyright and social engineering as well as digital footprints and online reputations. They will learn what to do should such a situation arise.

3. Managing internet access using school-based systems

3.1 Information system security

- The security and robustness of school-based systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Decisions surround security and strategies will be made by SLT and ICT support.

3.2 Managing filtering

- The school has developed its own comprehensive in-house filtering systems which have been deployed across the whole school network. These provide an infrastructure tailored to the school's particular needs and requirements. School will work with the local authority to ensure systems protect pupils and are reviewed and improved.
- Senior Leadership will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Pupils will be instructed to report unsuitable sites to the e-Safety Coordinator or their own teacher. The e-safety coordinator will investigate the site and, if necessary, liaise with network staff to ensure the site is blocked.

3.3 Email and messaging

Email / messaging are powerful and useful tools that have become an integral part of most young people's lives. They are not intrinsically harmful and can reduce isolation and encourage collaborative learning. However, we realise that systems can be used to bully and manipulate pupils and the following principles are at the core of the policy:

- When using the school system, pupils may only use approved email accounts.
- Pupils must immediately tell a member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- As part of an acceptable use agreement, pupils will undertake to never send hurtful or damaging messages to anyone in the school community regardless of the ownership of the device that the message is sent or received on. Older students will be reminded that the sending of abusive messages is illegal under the malicious communications act 1998.

3.4 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and the risks will be assessed. It should be realised that potential problems or harm may not emerge until after the adoption of a technology.
- The school will reassess the suitability of technology and systems over time and check that they remain suitable, secure, and effective.

4 Published content and Pupils

4.1 The school website

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The Head teacher with support from ICT will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.2 Publishing pupils' images and work on the web

Open / public sites

The school understands that public sites can be used to gather information and the locations of pupils. Written permission to use photographs and work on websites will have been obtained as part of the contract signed by parents. However, unless there is need to identify a pupil (e.g. to celebrate a prize) the following guidelines should be observed:

- School will have a robust procedure to determine that photographic permission for individual students is in place prior to any images being posted on-line
- Pupils' full names will not normally be used on the website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully. Care will be taken when taking digital/video images that pupils are appropriately dressed.

Closed/ Secure sites

Pupils' images, video, and work, can be made available to parents on secure areas of the web as long as the following measures are adhered to:

- The parents /carer should have a secure log-on to view the information on their pupils.
- Parents should be made aware that their child's images may be included in group work viewable by other parents /carers.

4.3 Social networking and personal publishing

- The school will block/filter access to social network and chat sites, depending on the way in which they are used and the characteristics they have.

  Pupils will be advised that social networking has potential dangers. As part of their acceptable use agreement, they will be told never to give out personal details of any kind which may identify them

or their location regardless of whether they are accessing the site from a school system or otherwise.

- Staff must use discretion when using social networking sites. They should ensure that their professionalism is maintained by refraining from "friending" past or present pupils even on a social level. They must not develop social relationships with any persons under the age of eighteen with whom they have had a professional relationship. Professionalism should be maintained to avoid any situations that may bring the school into disrepute

4.4 Using web sites with pupils

Pupils are often directed to internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing electronic world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- Sites used in school will be accessed as part of educational activities only. The selection of sites will be altered to reflect the ages and abilities of the pupils. Staff will review sites before they are first used to determine whether they are relevant and safe.
- All sites will be filtered via the local authority and school systems to minimize the risk of inappropriate material being accessed.
- If pupils are asked to make online accounts for access to materials, identifiable personal information will not be disclosed and only school e-mails with user names will be used.
- The school will be as open as possible about the sites and software it uses and welcome parents who wish to raise concerns or understand more about the way that ICT/Computing contributes to education.

It should be noted that because of differing laws (particularly in the USA) terms and conditions of some sites have apparent restrictions which do not apply in the UK. The school takes the view that "restricted" but innocuous sites with useful educational materials will be used unless concerns become evident.

5. <u>General provisions of the policy – Staff & Pupils</u>

5.1 Protecting personal data

Any recording, processing, or transfer of personal data will be carried out in accordance with the key principals of the Data Protection Act 1998.

5.2 Authorising internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement for Staff' before using any school ICT resource. Differing versions of this agreement may be used to match the personal and professional roles of staff members. A copy of this agreement will be given to staff member for their reference.
- All pupils will be introduced to the 'Acceptable ICT Use Agreement for Pupils' and the reasons for the rules will be explained to them. Pupils will be expected to abide by the agreement. The school

may decide to use different versions of this agreement to match the age group of the youngsters involved.

- Parents will be asked to sign an electronic consent form as part of the student's acceptable use agreement. Consent is maintained for the durations of a student's time at school. Parental consent is recorded under section 12 of the school's Information Management system (SIMS)
- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date. This will take account of changes such as a member of staff who has left the school or a pupil whose access has been withdrawn (in line DPA/GDPR 2018)

5.3 Staff use of Equipment and the Internet

The equipment provided for staff is primarily intended to support the teaching and learning of pupils. However, it is unreasonable to deny staff access to the internet for legitimate personal use (for example to contact a son or daughter's school). Nevertheless, discretion and the highest professional standards are expected of staff using school equipment.

Expectations are set out in the Acceptable Use Agreement for staff mentioned above, but will include:

- Keeping a proper professional distance e.g. must not "befriend" pupils on social networking sites.
- Being aware of the need for appropriate language and behaviour particularly when using messaging or e-mails.
- Not posting inappropriate material on websites which can be viewed by pupils or parents.

5.4 Assessing risks

The school will take all reasonable precautions to ensure that users abide by the acceptable use agreements and access only appropriate material.

The school cannot be liable for the consequences of staff or pupils deliberately breaking the acceptable use agreements which are published for their protection.

Due to the international scale and linked nature of internet content, it is also not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the agreements.

The school cannot accept liability for material accessed, or any consequences of internet access.

The school will periodically audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

Staff using ICT equipment will mainly be covered by the provisions of the Display Screen Equipment (Health and Safety) regulations 1992 amended 2002. Guidance, definitions, and requirements can be found on the HSE.

The use of DSE by pupils is not covered by the Display Screen Equipment Regulations. However, it is good practice to apply the requirements of the legislation to their workstations thus helping them to develop safe working practices.

5.4 Handling e-safety complaints

Complaints about ICT misuse by pupils will be dealt with by a senior member of staff under the procedures of the school and according to the nature of the complaint.

Any complaint about staff misuse must be referred to the Head teacher or another member of leadership.

Complaints of a child protection nature must be dealt with in accordance with statutory child protection procedures.

Pupils and parents will be informed of the school's complaints procedure.

5.5 Content, contact and conduct exemplar situations which may arise requiring intervention

	Commercial	**Aggressive**	**Sexual**	**Values**
Content (Child as a recipient)	Advertisements Spam Sponsorship Personal information	Violent/hateful content Lifestyle sites	Pornographic or unwelcome sexual content	Bias Racism Misleading information
Contact (Child as participant)	Tracking Harvesting/phishing Personal information	Cyber-bullied, harassed or stalked	Meeting strangers Grooming	Self-harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Terrorism Financial scams	Cyber-bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info and advice Health and wellbeing; time spent online

6. Communicating the policy

6.1 Introducing the e-Safety Policy to Children

- E-safety rules will be posted in all networked rooms and discussed with pupils at appropriate times throughout the school year. They will be in line with the policy and acceptable use agreements.
- Pupils will be informed that network and internet use will be monitored.

6.2 Staff and the e-Safety Policy

- All staff have access to an electronic copy of the e-Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

6.3 Enlisting parents' support

- Parents/carers attention will be drawn to the e-Safety Policy in newsletters, brochures and via the school website.
- Schools may decide to hold meetings to brief parents about e-safety policies and concerns.

7. Staff training

It is the responsibility of the school to provide staff with up to date training of E-Safety provisions arising from ongoing changes to mobile and computer based technologies

Available training provisions will be researched by the designated E-Safety coordinator and undertaken by all members of teaching and support staff.

The school will also ensure that at least one member of staff has been CEOP trained. The current member of staff who has fulfilled this requirement is Mr A. Didcote (Assistant Director for computing).

8. Review

Reviewed – October 2020

Review date – October 2022

9. Appendices

Dear Parent/ Carer

Acceptable Use / E-Safety agreement,

ICT (including the internet, email and mobile technologies) has become an important part of learning. Because of this, we feel that it is also important for young people to appreciate the rules around e-safety and the responsible uses of technology.

The attached agreement sets out some basic rules for staying safe and also covers the expectations that the school has about the way that pupils are expected to behave online.

Please could pupils read and discuss this agreement with their parent or carer. Signing the slip below shows that they understand (and will follow) the terms of the agreement. Any concerns can be discussed with their class teacher or Mr J Warren/Mr A Didcote, Stockport School E-Safety coordinator(s).

Please return the bottom section of this form to school for filing.

Internet sites and software at school

You will be aware that pupils are often directed to internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing electronic world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

1. Sites used in school will be accessed as part of educational activities only. The selection of sites will be altered to reflect the ages and abilities of the pupils. Staff will review sites before they are first used to ascertain whether they are relevant and safe.
2. All sites will be filtered via the local authority system to minimize the risk of inappropriate material being accessed. However, the interconnected nature of the web means that it is impossible to guarantee that this will never occur. A report from Ofsted has suggested that the opportunities to discuss instances of this sort in an educational environment increase the overall safety of pupils in the wider world. The school will always use incidents that arise to increase pupil's awareness of e-safety issues.
3. If pupils are asked to make online accounts for access to materials, identifiable personal information will not be disclosed and only school e-mails will be used.
4. The school will be as open as possible about the sites and software it uses and welcomes parents who wish to raise concerns or understand more about the way that ICT contributes to education.

It should be noted that because of differing laws (particularly in the USA) terms and conditions of some sites have apparent restrictions. It is not clear whether these restrictions apply in the UK. The school takes the view that "restricted" but innocuous sites with useful educational materials will be used unless concerns become evident.

Yours sincerely,

Mr I. R. Irwin
Headteacher

Pupil and Parent/Carer signature

We have discussed this document and ……..(pupil name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at Stockport School.

Parent/ Carer Signature …….

Pupil Signature…….

Form …….. Date ……

Pupil Acceptable Use Agreement / E-Safety Rules

Online behaviour

- ✓ I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- ✓ I will not download or install software on school ICT equipment without permission.
- ✓ I will only log on to the school network/ learning platform with my own user name and password.
- ✓ I will follow the school's ICT security system and not reveal my passwords to anyone.
- ✓ I will only use my school email address when using school devices.
- ✓ I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible. I will never post aggressive or offensive material on the system or the web at any time.
- ✓ I will respect the privacy and ownership of others' work on-line at all times.
- ✓ I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher
- ✓ I will not attempt to bypass the internet filtering system.
- ✓ I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent / guardian may be contacted.

Online Safety at All Times.

- ✓ I will be very careful about giving out personal information such as name, phone number or address online. I will not post my information in a social network profile so that anyone can see it.
- ✓ I will **not** arrange to meet someone I only know online unless my parent / guardian / teacher has clearly approved of this.
- ✓ I understand that online contacts may lie about their identity. I know that information on the web can be unreliable. I will be very cautious about who and what I believe.
- ✓ Images of pupils and / or staff will only be taken, stored and used for school purposes in line with school policy. I will not distribute images outside the school network without permission.
- ✓ I will support the school approach to online safety and not deliberately upload or send any text, images, video, or sounds that could upset or offend any member of the school community
- ✓ I understand that all my use of Stockport School's systems is monitored and logged and can be made available to my teachers.
- ✓ If anything makes me uncomfortable or worried, I know that I can share this with a teacher or parent without being blamed.