SCSP

Steel City Schools Partnership

SCSP

Online Safety Policy

Responsibility	SCSP
Date of last review	September 2019
Date of next review	September 2020

Contents

At Steel City Schools Partnership, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst SCSP 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 has been created with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. We are committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- The General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997
- SSCB Safeguarding Children Board Safeguarding Policies 2019

This policy also has regard to the following statutory guidance:

- DfE (2018) 'Keeping children safe in education' annex C

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

- Social Media Policy
- Staff Acceptable Use Agreement
- Pupil Acceptable Use Agreement
- GDPR Policy and associated privacy notices

Use of the Internet

The purpose of Internet use at SCSP is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance SCSP's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. SCSP has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils world-wide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority and DfE
- access to learning wherever and whenever convenient

Ways in which the Internet can enhance learning include:

- SCSP Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Roles and responsibilities

- It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the academy, and to deal with incidents of such as a priority.
- SCSP and each academy is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.
- Each academy will have a designated Online Safety Coordinator who is responsible for ensuring the day-to-day online safety in the academy, and managing any issues that may arise.
- SCSP is responsible for ensuring that the online safety officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

- The online safety officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.
- SCSP will ensure there is a system in place which monitors and supports the online safety officer, whose role is to carry out the monitoring of online safety in the academy, keeping in mind data protection requirements.
- The online safety officer will regularly monitor the provision of online safety in the academy and will provide feedback to both SCSP and the academy principal.
- Each academy will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.
- Cyber bullying incidents will be reported in accordance with the Anti-Bullying Policy.
- Trustees and academy governors will review the effectiveness of the online safety provision, current issues, and to review incident logs, as part of their duty of care.
- Teachers are responsible for ensuring that online safety issues are embedded in the curriculum and safe internet access is promoted at all times.
- All staff are responsible for ensuring they are up-to-date with current online safety issues, and this policy.
- All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement. The pupil agreement will be shared and displayed for pupils.
- Each academy is responsible for communicating with parents regularly and updating them on current online safety issues and control measures.
- All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

Online safety education

Education children:

- An online safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the academy.
- Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be available for pupils.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- Academies may hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

Education for staff:

- Online safety training opportunities will be available to all staff members, including whole school activities, craft of teaching and CPD training courses.
- All staff will undergo online safety training alongside safeguarding training to ensure they are aware of current issues and any changes to the provision, as well as current developments in social media and the internet as a whole.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

- All staff will be advised on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff will be advised about online safety and safeguarding as part of their induction, ensuring they fully understand this Online Safety Policy.
- The online safety coordinator will act as the first point of contact for staff requiring advice.

Educating families:

- Online safety information will be directly delivered to families through a variety of formats, including newsletters, the academy websites, social media, leaflets and workshops.
- Families will be made aware of who the Online Safety Coordinator is should they require any advice or support.

Online safety control measures

Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils’ activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils’ age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- All staff and pupils should be aware that internet use will be filtered and automatically monitored when accessing online content through the academy network (both wired and wireless). Any inappropriate use may be flagged up by the filtering system.
- The Trust will ensure that use of appropriate filters and monitoring systems does not lead to ‘over blocking’, such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Principal and/or Online Safety Coordinator.
- All systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers, guests etc.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Staff should be aware that any personal use will also be automatically filtered and monitored by the filtering system. This will only be monitored if access to any inappropriate or explicit sites is flagged which would outweigh the need for privacy.

Email:

- Pupils may only use approved email accounts on SCSP's systems.
- Pupils must immediately tell a teacher 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.
- Access to external personal email accounts may be blocked while on SCSP property.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on SCSP headed paper.

- Staff may contact pupils via approved SCSP email accounts as this can be monitored by the e-safety coordinators. This should be within school hours and only be about school related work.
- Any information sent via email will be in line with our GDPR Policy and guidelines. This includes using password protection and encryption, not revealing too much personal information etc.
- Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages are not monitored.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Pupils and staff will be advised that chain letters, spam and all other emails from unknown sources should be deleted without opening.

Social networking:

- SCSP will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised about the rules of using social networking sites and we aim to educate children about the legal implications of improper use.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Staff are advised to use security settings within their social networking site to restrict information to only known friends. Staff can see the e-safety coordinator for help with this.
- It is not appropriate for staff to share work-related information whether written or pictorial via a social networking site.
- Under no circumstance should comments be made about other staff, pupils, parents/carers or school procedures on the Internet. Staff members should respect the privacy and the feelings of others. This could be deemed a disciplinary offence.
- SCSP staff should not be friends with parents, carers or pupils on social networking sites. In situations where staff are friends with parents in a social capacity, it may be necessary for separate accounts to be held.
- If a member of staff believes something has been written which gives rise to concerns within this, or any other policy this must be discussed with the e-safety coordinator and a member of the Senior Leadership team.
- If a message or 'friend request' is received by a member of staff from a parent, carer or pupil, staff should ignore any messages and reject the request. Under no circumstances should staff reply as this can result in online information becoming available to others. Staff should inform the school e-safety coordinator about any messages or friend requests received from parents, carers or pupils.

Published content on the school website and images:

- Each academy will be responsible for the overall content of the website, and will ensure the content is appropriate, accurate and in line with SCSP guidelines and policy.
- Contact details on the academy website will include the phone number, email and address of the academy – no personal details of staff or pupils will be published.

- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with the policies in terms of the sharing and distribution of such. Staff will 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.
- All online content will be compliant with the GDPR policy and procedures.

Mobile devices and hand-held computers:

- SCSP and the academy may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the academy Wi-Fi system at any time using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils. If brought into the academy, these will be stored in line with the SCSP Mobile Phone Policy.
- Staff are permitted to use hand-held computers which have been provided by the school, though staff should be aware that all internet access will be monitored via the academy filtering system.

Video conferencing:

- Video conferencing will always be done through an approved provider and will always be fully supervised.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the pupils' ages.

Network security:

- Network profiles for each pupil in KS2 and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Network drives and information are organised in such a way that users only have access to relevant information that they are allowed to access in line with the GDPR Policy.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and The General Data Protection Regulation (GDPR).

Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the Online Safety Officer.
- The Online Safety Officer at each academy will ensure that the filtering of websites and downloads is up-to-date and monitored. This will be done in liaison with the technical support services.
- Staff will be kept up-to-date on any virus threats which could threaten their own computer use and that of SCSP.

Cyber bullying

- For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online. This is in line with the Anti-bullying Policy.
- SCSP recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
- SCSP will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- Pupils will be 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 sex and relationship education.
- SCSP commits to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- SCSP has zero tolerance for cyber bullying, and any incidents will be treated with the utmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

Assessing Risks

- SCSP will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a SCSP computer. Neither SCSP nor Sheffield City Council can accept liability for the material accessed, or any consequences of Internet access.
- SCSP will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the online safety coordinator and a member of the SLT. If a data protection breach, this must be reported to the academy data controller or a member of the SLT.
- Complaints of a child protection nature must be dealt with in accordance with SCSP child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of policy

Children:

- Rules for Internet access will be posted around the academy buildings.
- Pupils will be informed that Internet use will be monitored.
- Pupils will have read and have access to the online safety rules.

Staff:

- All staff will be given the SCSP Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Filtering systems in place automatically monitor all devices connected to the academy networks (including Wi-Fi) and staff should be mindful of this.

- Discretion and professional conduct is essential.
- Staff will have read and signed the Information Systems Code of Conduct and be aware of other associated policies such as the SCSP Social Media Policy, GDPR Policy etc.

Parents:

- Parents' attention will be drawn to SCSP Online Safety Policy in newsletters, the prospectus and on the academy web sites.
- They will have been asked to read our safe internet use rules and sign the home-school agreement.