SOUTH HUNSLEY

Online Safety Policy

This policy is applicable to: South Hunsley School
Intended audience: Staff, Parents, Students

Important: This document can only be considered valid when viewed on the school website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	Tom Sergeant, Assistant Headteacher
Name of Responsible Committee/Individual:	South Hunsley School and Sixth Form Local Governing Body
Implementation Date:	Spring 2020
Review Date:	Spring 2021
Target Audience:	All Staff, Parents, Students

Online Safety Policy

Contents

Introduction

The use of technology continues to be an important component of safeguarding young people. Technology, whilst providing many opportunities for learning also provides a platform that can facilitate harm. Keeping Children Safe in Education categorises online safety into three broad areas:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **Contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

It is with these three categories in mind that this policy outlines the roles, responsibilities and procedures for ensuring online safety.

Aims

This policy aims to set out the school's position in how it will strive to provide a safe environment for all of the school community whilst using ICT within the school, and how it will also strive to ensure that its members also use ICT, including their own personal devices, in a safe and responsible manner whilst outside of the school grounds.

This policy will detail the individual responsibilities of each of the key people in the school who have a role to play in fulfilling this policy and its related procedures.

This policy applies to all staff, students, governors and parents of the school community. It should be read in conjunction with the supporting policies and related information that is detailed below.

South Hunsley School believes that ICT can and should be used to enrich the education of all students. ICT also provides the staff of the school with a great many tools to help them play their part in providing the students of the school their education. Whilst the school sees the benefits of using this technology, it is also aware of the potential risks that the internet, ICT and related technology can pose. The school believe that online safety is the responsibility of the whole school community, and that all members of that community have their own part to play in ensuring that everyone can gain from the benefits that the internet and ICT afford to teaching and learning, whilst remaining safe.

Social Networking is becoming an increasingly popular tool within our environment to support learning, encourage creative and appropriate use of the internet and to publish and share content. These technologies need to be used in a safe and responsible way, and appropriate online behaviour encouraged. Although we encourage staff to use social networking to promote learning within school, we also expect staff to maintain a professional level of conduct in their use of these types of technologies.

Risks & Responsibilities

Risks of ICT use and the Internet

The school has identified the following risks that ICT and the internet can pose to its community: [1]

- Obsessive use of the internet and ICT

[1]This list is by no means exhaustive, but means to highlight some of the main areas of risk that the school has identified.

- Exposure to age inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger or sexual abuse
- Being subjected to harmful online interaction with other users
- Inappropriate or illegal behaviour by school staff
- Actions that bring the school into disrepute
- Online grooming or child exploitation

Creating a Safe ICT Learning Environment

The school believes that the best way to provide a safe ICT learning environment is a triple-fold matter:

1. Create an infrastructure of **whole-school awareness**, **designated responsibilities**, **policies and procedures**. This is achieved by:
    - Raising awareness of the risks of ever-changing technology that is both emerging and already embedded in the school community.
    - Ensuring that the Online Safety policy and education programme adapts to meet these new and emerging technologies and is reviewed as incidents occur.
    - Establishing a clear understanding of the responsibilities of all of those involved with the education of children, with regards to Online Safety.
    - Ensuring that the school's policies and procedures are effective and kept up to date, and also make clear to all members of the school community what is acceptable when using ICT and the internet.
2. Make use of **effective technological tools** to ensure the safe use of the internet and school ICT systems. These include:
    - Firewall protection to the school's network.
    - Virus protection of all relevant IT equipment connected to the school's network.
    - Filtering, logging and content control of the school's internet connection.
    - Monitoring systems.
3. Develop an **Online Safety education programme** for the whole school. This will consist of:
    - An on-going education programme for the students at the school, so that they are given the tools to formulate and develop their own parameters of acceptable behaviour and take these with them when they leave the school.
    - Continued Professional Development for staff to ensure that they are equipped to support the students at the school, and are also fully aware of their responsibilities in using ICT, both in and out of the school.
    - An on-going education programme for parents, carers and the wider community so that they have the knowledge and tools available to support the actions of the school in these matters.
    - Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.
    - Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
    - Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.
    - Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.

- Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.

Headteacher's Responsibilities

1. To take ultimate responsibility for online safety whilst delegating the day-to-day responsibility to the Online Safety Coordinator (OSC).
2. To ensure that the OSC and the members of the online safety teams are given enough time, support and authority to carry out their remit.
3. To ensure that the governing body is kept informed of the issues and policies.
4. To ensure that the appropriate funding is available to support the technological infrastructure and CPD training for the online safety programme.

Governing Body's Responsibilities

1. To ensure the \designated Safeguarding Governor considers online safety as a part of the regular review of child protection and safeguarding.
2. To support the Headteacher and OSC to ensure that the correct policies and procedures are in place, and also that the funding required to achieve these policies and procedures is available.
3. To help in the promotion of online safety to parents.

Online Safety Coordinator's Responsibilities

1. To develop and review the appropriate online safety policies and procedures.
2. To develop management protocols so that any incidents are responded to in a consistent and appropriate manner.
3. To work with the appropriate members of staff to develop a staff CPD programme to cover all areas of online safety inside and outside of the school environment.
4. To work with the appropriate members of staff to develop an online safety education programme for the students.
5. To work with the appropriate members of staff to develop a parental awareness programme for online safety at home.
6. To maintain a log of all online safety incidents that occur in the school.
7. To recommend reviews of technological solutions, procedures and policies based upon analysis of logs and emerging trends.
8. To meet with the Child Protection Officer regularly to discuss online safety and progress.
9. To liaise with any outside agencies as appropriate.
10. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Child Protection Officer's Responsibilities

1. To seek professional development on the safety issues relating to the use of the internet and related technologies, and how these relate to young people.
2. To liaise with the OSC on specific incidents of misuse.
3. Take a proactive role in the online safety education of the school's students.
4. Develop systems and procedures for supporting and referring students identified as victims or perpetrators of online safety incidents.
5. To maintain an appropriate level of professional conduct in their own internet use, both within and

outside the school.

IT Manager Responsibilities

1. To perform regular audits and checks of the school's networked systems to look for signs of misuse or inappropriate files. Any such findings would need to be reported to the OSC, Headteacher and Police if necessary.
2. Review the technological systems upon any discovery or breach of the Acceptable Use Policy (AUP), to ensure that the same breach does not happen again.
3. Liaise with the pastoral team if any breach can be traced back to an individual student.
4. Liaise with the OSC and Headteacher if any breach can be traced back to an individual member of staff.
5. Provide the technological infrastructure to support the online safety policies and procedures.
6. Report any network breaches of the school's Acceptable Use Policy or online safety Policy to the OSC.
7. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Subject Leaders' Responsibilities

1. To work with the OSC to develop an area / departmental policy to ensure that online safety is embedded in their areas teaching practice, where appropriate.
2. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.
3. To alert the OSC to the creation of any school social media accounts.

Heads of House Responsibilities

1. To act as a key member, and first point of contact for the school's online safety team.
2. To support the OSC in the development and maintenance of appropriate policies and procedures relating to student welfare.
3. To develop and maintain their own knowledge of online safety issues.
4. To ensure that any incidents of ICT misuse are dealt with through the correct channels, in line with the ICT Acceptable Use Policy, Behaviour Policy and Online Safety Policy.
5. To ensure that any students who experience problems when using the internet are appropriately supported, working with the OSC and CPO as required.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Special Educational Needs Coordinator's Responsibilities

1. To develop and maintain a knowledge of online safety issues, with particular regard as to how they may affect children and young people with additional educational needs.
2. To develop and maintain additional policies and online safety materials in conjunction with the OSC, tailored to meet the needs of SEN students.
3. To liaise with parents and carers of SEN students to raise awareness of the school's online safety position and how the parents can support the school's position.
4. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Classroom Teachers, Teaching Assistants, LRC Staff and Cover Supervisors' Responsibilities

1. To develop and maintain a knowledge of online safety issues, with particular regard to how they might

affect children and young people.

2. To implement school and departmental online safety policies through effective classroom practice.
3. To ensure any incidents of ICT misuse are reported through the correct channels.
4. To ensure that the necessary support is provided to students who experience problems when using the internet, and that issues are correctly reported to the OSC and the pastoral team.
5. To plan classroom use of ICT facilities so that online safety is not compromised.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.
7. To alert the OSC to the creation of any school social media accounts

Student's Responsibilities

1. To uphold all school online safety and ICT policies.
2. To report any misuse of ICT within the school to a member of staff.
3. To seek help or advice from a teacher or trusted adult if they, or another student experience problems online.
4. To communicate with their parents or carers about online safety issues and to uphold any rules regarding online safety that may exist in the home.

Parents' and Carers' Responsibilities

1. To help and support the school in promoting online safety
2. To discuss online safety concerns with children and to show an interest in how they use technology.
3. To take responsibility for learning about new technologies and the risks they could pose.
4. To model safe and responsible behaviour in their own use of the internet.
5. To discuss any concerns they may have about their children's use of the internet and technology with the school.

Procedures & Implementation

The school, through the Online Safety Coordinator, will ensure that all staff are aware of the policies and procedures being implemented to meet the Online Safety remit. There will be information available to all staff about the technologies that are already in use at the school as well as new and emerging technologies that they may come across in their professional practice. All staff will be given the opportunity to feedback into the school's online safety discussions, be given clear guidance to what the procedures are and know who they should speak to regarding any issues.

In the first instance, all staff will receive a basic introduction into the online safety programme at the school, and be directed towards the resources that have been made available.

An area of the Virtual Learning Environment contains relevant resources and links to information regarding the safe use of new technologies within a school environment. This area also contains documentation of all people's roles with regards to online Safety in the school and a clear flowchart of the correct procedures to follow.

The OSC will work with the HR Team and Assistant Headteacher responsible for CPD to ensure that the school's induction and CPD programmes include adequate provision for the delivery of online safety training.

Online safety will form a part of the Child Protection Induction for new staff starters and direct them towards the existing policies, procedures, resources and courses of action.

Students

The students at the school will be made aware that there is a whole school approach to online safety and their roles and responsibilities within this e-Safe environment will be made clear to them. Student members will be invited to participate in the future planning and discussions regarding online safety and their opinions will be regularly gauged as to the effectiveness of the provision.

Through individual House assemblies, students will be made aware of policies and methods of enforcing these policies.

The Year 12 students will be made aware of the school's position regarding online safety in their LRC induction programme. A follow-up assembly will be held for all Year 13 students to make them aware and refresh their understanding.

Parents and Carers

The parents and carers of the school will be made aware of policies and procedures and how they can help in ensuring that South Hunsley is an e-Safe school. We will ensure that parents and carers can access information regarding the risks of new technologies, but also how they can ensure these technologies are being used safely.

An area on the school's Virtual Learning Environment contains useful links and information for parents and carers regarding online safety. This area will also contain links to the school's online safety policy, the ICT AUP and the Child Protection Policy.

Parental workshops will be delivered to give parents the opportunity to understand online safety topics and new risks children are opposed to.

Firewall

The school has a perimeter firewall, which is supplied by Smoothwall. This physical hardware device sits at the edge of the network and allows only specific traffic in and out of the network. All intrusion attempts from both sides of the network can be logged and analysed for security audits.

The responsibility lies with the IT Manager for ensuring that the firewall is correctly configured and that intrusion logs are regularly checked.

Anti-Virus Protection

The school has purchased a third party security suite from Heimdal Security, which compromises a number of security tools to protect our network including; anti-virus, auto patching applications and malware redirect detection. The school also have an Enterprise License for Microsoft's Endpoint Protection. This anti-virus software is installed on Microsoft Windows based servers that are not being supported by Heimdal Security. The VLE web server has ClamAV installed and all uploaded files are scanned for viruses before being accepted onto the servers.

It is the responsibility of the Deputy IT Manager to ensure that all necessary computers on the school network are running current anti-virus software and that regular scans are performed. If a virus out-break happens, the Deputy IT Manager must notify the IT Manager and the Headteacher and as soon as possible isolate the infection.

Personal devices for staff and sixth form should connect to the **sh-users** network using their computer credentials to authenticate, this wireless network is ring-fenced by a firewall to protect internal network devices and only allow certain internal applications to connect. Visitors must obtain a key from the IT Support team or reception and use the **sh-visitor** wireless network, which is a less filtered connection to provide guests an internet connection, secure sites are also not logged on this wireless network. Any devices being brought into to school and connected to the school's ICT network via Ethernet to obtain a wired connection to the network must be proven to have up-to-date Anti-Virus protection and be cleared by the Deputy IT Manager or IT Manager before being connected.

Filtering and Logging of Internet Access

The school has a web caching and proxy server that contains accredited filter lists. This enables the school to

log all Internet traffic in the school and allow different sites to different groups of users. This server ensures that all internet use on the school's network is logged to an individual user of the network. If the device being used to access the Internet is not a school owned device, the user will have to present valid school network credentials before they can gain any access to the school's Internet connection. If an online safety incident requires it, all Internet access logs of any student or staff member can be retrieved to support any required processes.

It is the responsibility of the Deputy IT Manager to ensure that all computers connected to the school's network only receive an Internet connection by going through the proxy server. The Deputy IT Manager, on request of the OSC, will add any sites that have been discovered through online safety incidents to the block lists of the filtering server. The Deputy IT Manager will perform regular reports from the logs of the web proxy server to present to the OSC and IT Manager, with regards to the most accessed sites and most active Internet users in the school.

Monitoring Systems

The school has many different monitoring system at its disposal;

- All files stored on the school's servers can be searched and checked
- Teachers can monitor the students use of computers within the IT labs they are in
- Every single action performed on the VLE is logged against the user that performed the action. These logs can be accessed to provide evidence for an online safety incident
- All computer use is monitored centrally against a set of predefined word lists and use or viewing of inappropriate text is logged with a screen grab and the details of the offence, user and time it occurred
- Any incident that has a sanction attached to it is entered into the school's MIS system
- Computer use is live monitored using Smoothwall Monitor Managed Service with incidents alerted to the OSC, CPO and IT Manager

The Deputy IT Manager will perform a scan of all staff and student home drives for all images and identify any inappropriate images saved. This will be performed once every term and any inappropriate images found, the Deputy IT Manager will notify the OSC providing the user name involved, full name of the user, date and time discovered, details of the incident or violation.

The Deputy IT Manager will review all users profile pictures, blog entries on the VLE and Office 365 sites. This will be performed once every term and any inappropriate images found, the Deputy IT Manager will notify the OSC providing the user name involved, full name of the user, date and time discovered, details of the incident or violation.

Training in the use of the IT monitoring software will be offered to all staff. The procedure for reporting online safety incidents will detail the information needed from staff when reporting an incident recorded by this software.

The monitoring system will monitor all users (staff and students) the same and the client will be installed on all school owned computers. The difference between staff and students, with regards to this monitoring system, will be the method in which those logs are reviewed.

The Deputy IT Manager and OSC will access and review the logs of the silent monitoring system for the staff and respond accordingly to any breaches of the AUP or other online Safety incidents recorded.

Any incident that has a sanction attached will be entered into the SIMS system using the behaviour type of **ICT AUP Breach**. These incidents can then be reported upon and shared with relevant Head of House and Subject Leaders as required.

Where incidents raise concern regarding a child's welfare they will be also recorded on our online Child Protection Monitoring System CPOMS where a pattern of concern can be identified if appropriate.

Currently, school-owned iPads do not have individual monitoring on them, as due to the nature of the device, you cannot identify the user at any given time. As such, they are filtered through the web proxy with the most restrictive policy applied.

Online Safety Education

All students at the school will receive an on-going online safety education programme.

This programme will inform the students of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments as new technology is adopted. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

The ICT & Computing department run a distinct six-week e-Safety unit with every Year 7 student through their weekly ICT lessons. The content of these lessons is regularly reviewed to include up to date issues. Currently the unit is developed in line with DfE guidance and covers:

- Content Risks:
  - Identifying fake content
  - Risks associated with social media (violence, hate speech, pornography, etc.)
- Contact Risks:
  - Grooming
  - Image sharing
  - Scams
- Conduct Risks:
  - Web archiving & Digital footprints
  - Bullying
  - Obsession & Self Image

The School's PSHE curriculum is under constant review to include emerging trends in students' online use and to address new uses as they arise. Currently this covers:

- Staying Safe Online – Year 7
- Sexting & Sexual Exploitation Online – Year 9

The school will follow the Safer Internet Day programme and deliver those resources through House assemblies. Form tutors will be informed about the content being delivered, and asked to discuss the content after the assembly is given so that students have an opportunity to raise any concerns or issues from this information.

The Post-16 team will work with the OSC to ensure that there is an adequate online Safety education programme within the Post-16 Curriculum, and that the pastoral support team are up to date with the issues within their area. The online safety education programme will be delivered through the Post-16 PSHE programme.

The PSHE and Personal Development curriculum will be regularly reviewed to ensure that it has appropriate and relevant online safety content incorporated into its programme.

The SENCO will work with the OSC to ensure that there are accessible and adequate resources available for SEND students of the school to access the same online safety education as the rest of the school.

Responding to a concern

Appendix 1 outlines the process regarding concerns being raised relating to online safety. In the first instance any concern should be reported to the student's Head of House.

As a school, we proactively work to ensure the safety of our students both in-school and online. We do not have the capacity to police all online activity outside of school, however where actions of a student online go against our code of conduct, as outlined in the School's Behaviour Policy, we will sanction students, following the expectations set out in Section 7 of our Behaviour Policy.

Where actions taken by students online pose a risk to them or others, they will be dealt with in line with our Child Protection Procedure, conducting appropriate risk assessments and ensuring minimal disruption to any victim, where appropriate.

Consistent Approach

The OSC will work with the pastoral team to ensure there is a commonality of approach in responding to online safety incidents and that the correct reaction and procedure is followed by all staff when dealing with an online safety issue.

School Social Media Accounts

The school will support departments wishing to set up social media accounts.

Whilst all social media is different, and constantly evolving there are some key expectations for colleagues using social media in school, which are as follows:

- Any colleague wishing to set up a school or departmental social media account should first seek approval from the OSC and reasons behind the decision.
- All social media must be set up to ensure that that there can be no private communication or Direct Messaging between the account and the accounts of students.
- A log of all social media accounts in school should be kept by the OSC.
- Passwords should not be shared between colleagues and one colleague should take overall responsibility for the account and its content.
- Users should follow the expectations and responsibilities of colleagues outlined above.

As stated above, social media is constantly changing and as such advice should be sought from the OCS and IT Manager where appropriate.

Supporting Policies and Related Information

South Hunsley School and Sixth Form College/Education Alliance supporting policies:

- ICT AUP
- Child Protection Policy & Procedure
- Expectations and Code of Conduct for Staff
- Prevent Policy
- Student Behaviour Policy

Procedure for Policy Implementation

The procedural document for this policy is attached as an appendix.

- Appendix 1 – Online Safety Incident Reporting Flowchart

Appendix 1 - Responding to incidents of misuse (Flow Chart)