



Online Safety Policy

Policy Reference:

To be reviewed by: April 2022

Policy Owner: Richard Potter

Policy Progression Revisions

Date	Reviewed by	Description of changes
April 2021		New Policy

Date Approved	
Date Reviewed by	
Signature of Chair	
Print Name	

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school	7
8. Pupils using mobile devices in school	7
9. Staff using work devices outside school	8
10. How the school will respond to issues of misuse	8
11. Training	8
12. Monitoring arrangements	9
13. Links with other policies	9
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	10
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)	11
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	12
Appendix 4: online safety training needs – self audit for staff	15
Appendix 5: online safety incident report log	16

1. Aims

Sir Harry Smith Community College aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet. (appendix 3)

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL [and Deputies] are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3) and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)
- [Healthy relationships – Disrespect Nobody](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#).

The introduction of the new relationships and sex education (RSE) curriculum was compulsory from September 2020 as planned for schools who were prepared to deliver it – but:

Under the new requirement, **all** schools will have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

This new requirement includes aspects about online safety. As such we've added these expectations in italics below.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*

- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Justine Henderson Trust Operations Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and / or acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Acceptable Use Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils)

SHSCC STUDENT ACCEPTABLE USE AGREEMENT

Name of pupil:

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the College's computers for College work, homework and as directed.
2. I will not bring files into College (on removeable media or online) without permission or upload inappropriate material to my workspace (including games). I will only edit or delete my own files and not view or change other people's files without their permission.
3. I will keep my logins, IDs and passwords secret.
4. I will use the Internet responsibly and will not visit websites I know to be banned by the College. I am also aware that during lessons I should only visit websites that are appropriate for my studies.
5. I will not use the College devices or College network for online gaming.
6. I will only email people I know or those approved by my teachers.
7. The messages I send, or information I upload, will always be polite and sensible.
8. I will not open attachments or download a file unless I have permission to or I know and trust the person that has sent them.
9. I will not give my home address, phone number, send photographs or video or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room unless I have a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message I do not like I will not respond to it but I will save it and talk to a teacher/trusted adult.
12. I am aware that some websites and social networks have age restrictions and I should respect this.
13. I am aware that my online activity, at all times, should not upset or hurt other people and I shouldn't put myself at risk.
14. I understand that sanctions may apply, if I was to go against this agreement.
15. I am aware that it is my responsibility to talk to a teacher/trusted adult if I become aware of any online activity that may impact other students and/or staff at SHSCC.

I have read and understood these rules and agree to them.

Signed (pupil):

Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

1. Trust Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

1.1 This Acceptable Use Policy is intended to ensure a. that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

b. that Trust systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

c. that staff are protected from potential risk in their use of technology in their everyday work. The Trust will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students/ pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

1.2 Acceptable Use Policy Agreement

I understand that I must use Trust systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

a. I understand that the Trust will monitor my use of the school digital technology and communications systems.

b. I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

c. I understand that the Trust digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school

d. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

e. I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Trust ICT systems:

a. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

b. I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

c. I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

d. I will only use social networking sites in school in accordance with the school's policies. e. I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. f. I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

a. When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using Trust equipment. I will also follow any additional rules set by the Trust about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

b. I will not use personal email addresses on the Trust ICT systems.

c. I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

d. I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.

e. I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

f. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

g. I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.

h. I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.

i. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

j. I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.

k. I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

a. I will ensure that I have permission to use the original work of others in my own work b. Where work is protected by copyright, I will not download or distribute copies (including music and videos).

b. I understand that I am responsible for my actions in and out of the Trust: I understand that this Acceptable Use Policy applies not only to my work and use of Trust digital technology equipment in school, but also applies to my use of Trust systems and equipment off the

premises and my use of personal equipment on the premises or in situations related to my employment by the Trust. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or Trustees and in the event of illegal activities, the involvement of the police. I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:.....

Signed:.....

Date:.....

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident