Online Safety Policy

Southend High School for Girls Academy Trust

Southend High School for Girls Academy Trust

Governor Policy 25NS	**Author:**	**Authorised by:** **Board of Governors**
Online Safety Policy	**Date first issued** **September 2017**	**Page 2 of 11**

Reviewing authority:

Date for review	Reviewed Annually by	Reviewed by Board	A	B	C	Date of new edition
Sept 2017	Full Governors	26/09/2021			*	26/09/2021
Sept 2021	Full Governors	07/09/2021			*	07/09/2021

A = accepted with no amendments

B = accepted with amendments

C = new edition created

Contents

1. AIMS

Southend High School for Girls aims to:

- Have robust processes in place to ensure the online safety of the school community
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2023, 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 and health 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 students' electronic devices where they believe there is a 'good reason' to do so.

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.

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

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.

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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS 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
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students 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 weekly/fortnightly/monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff are responsible for:

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use
- Working with the safeguarding team to ensure that any online safety incidents are reported 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

SHSG recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- Requesting that they read online safety information as part of our home school agreement.

Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.

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

4. REDUCING ONLINE RISKS

Southend High School for Girls will ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material. All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which would cause harm, distress or offence to members of the community. This is outlined in the staff code of conduct and acceptable use policies.

5. EDUCATING STUDENTS ABOUT ONLINE SAFETY

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

In **Key Stage 3**, students 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

Students 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**, students 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. The school will make use of support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

5.1 Vulnerable Students

SHSG is aware that some students are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND), health conditions or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. SHSG will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students. SHSG will seek input from specialist staff as appropriate, including the SENCO, LAC Lead.

6. EDUCATING PARENTS ABOUT ONLINE SAFETY

The school will raise parents' awareness of internet safety in communications home, and in information via our website. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Pastoral Support Officer.

7. CYBER-BULLYING

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.)

7.1 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. 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.

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 students, 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.

8. 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 students' 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
- Breach the school's behaviour and rewards policy

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 students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation

For incidents of students sharing nude or semi nude images or receiving indecent images, steps in the school's Safeguarding and Child Protection Policy should be followed and images must not be viewed.

9. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

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. Please refer to the staff code of conduct for more details.

10. SECURITY AND MANAGEMENT OF INFORMATION SYSTEMS

The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- The appropriate use of user logins and passwords to access the school network.
- Specific user logins and passwords will be enforced for all
- All users are expected to log off or lock their screens/devices if systems are unattended.

11. MANAGING PERSONAL DATA ONLINE

Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 2018.

12. STUDENTS USING MOBILE DEVICES IN SCHOOL

Please refer to the Mobile Phone Policy (students).

13. STAFF WORK DEVICES

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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- 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.

If staff have any concerns over the security of their device, they must seek advice from ICT manager.

14. SCHOOL EMAIL

Access to school email systems will take place in accordance with Data protection legislation. All staff members are provided with a specific school email address to use for all official communication. Students will use school email accounts for educational purposes. Please refer to the staff code of conduct and student acceptable user policies for further details.

15. USE OF SOCIAL MEDIA

All members of the SHSG community are expected to engage in social media in a positive, safe and responsible manner, at all times. All members of the SHSG community are advised not to publish pictures or messages on any social media services that may be considered indecent, threatening, hurtful or defamatory to others. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct. Please refer to this document for further information.

Staff will not use personal social media accounts to make contact with students or parents, nor should any contact be accepted. Any communication from students and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

Safe and appropriate use of social media will be taught to students as part of PSHE lessons. Where appropriate, concerns regarding students' use of social media will be dealt with in accordance with existing school policies, for example the Behaviour and Rewards policy and the Child Protection and Safeguarding policy.

Students are advised:

- To consider the risks of sharing personal details on social media sites which could identify them and their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer's permission
- To use social media sites which are appropriate for their age
- How to block and report unwanted communications and report concerns both within school and externally.

The official use of social media sites by the school only takes place once approved by the Headteacher. Only school staff will have administrative rights on official school social media channels.

16. LEARNING PLATFORMS

Southend High School for Girls uses Office 365 and Microsoft Teams as its official learning platforms.

- Only current members of staff and students will have access to these platforms.
- When staff and/or students leave the school, their account or rights to specific school areas will be disabled.
- Students and staff will be advised about acceptable conduct when using these platforms.
  Please refer to the Remote Teaching and Learning Policy for further details.

17. RESPONDING TO ONLINE SAFETY INCIDENTS

For incidents of inappropriate use of technology including the school's ICT systems of internet, the school's Behaviour and Rewards Policy will be followed. For specific safeguarding, child protection or bullying concerns, procedures in the Safeguarding and Child Protection Policy/Anti Bullying Policy will be followed. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Please refer to these policies for further details.

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/staff code of conduct. 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 or criminal activity or illegal content, or otherwise serious incidents, should be reported to the police.

18. TRAINING

All new staff members will receive training, as part of their induction, on 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 staff briefings).

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.

Staff will be made aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.

19. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-Bullying Policy
- Mobile Phone Policy (students)
- Staff Code of Conduct
- Data protection policy and privacy notices
- ICT and internet acceptable use policy
- Curriculum policies, such as: Relationships and Sex Education (RSE)
- The Remote Teaching and Learning Policy