

# ICT Acceptable Use Policy for Students

Southend High School for Girls Academy Trust



## Southend High School for Girls Academy Trust

<b>Governor Policy 5NS (ii)</b>	<b>Author:</b>	<b>Authorised by:</b> <b>Board of Governors</b>
<b>ICT Acceptable Use Policy for Students</b>	<b>Date first issued</b> <b>June 2021</b>	<b>Page 2 of 6</b>

**Reviewing authority:**

<b>Date for review</b>	<b>Reviewed Annually by</b>	<b>Reviewed by Board</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>Date of new edition</b>
<b>Jun 2021</b>	<b>S&amp;C</b>				<b>*</b>	<b>01/06/2021</b>
<b>Sep 2021</b>	<b>S&amp;C</b>			<b>*</b>		<b>07/09/2021</b>

**A = accepted with no amendments**

**B = accepted with amendments**

**C = new edition created**

## ICT Acceptable Use Policy for Students

SHSG values the use of technology and encourages its use in creative ways to support student learning in a safe and secure learning environment. To ensure that this occurs, the school community needs to be clear as to what is not acceptable.

Quite specifically, the following actions are not permitted:

- sending or displaying offensive messages or pictures from or to any device
- using obscene language
- cyber-bullying, harassing, insulting or attacking others
- damaging computers, computer systems, computer networks, electronic devices or other peoples files (for example, by the creation, introduction or spreading of computer viruses, physically abusing hardware, altering source codes or software settings, deleting, changing or printing other people's files etc.)
- avoiding or trying to avoid the school's filtering system
- installing or trying to install programmes of any type on any school device, nor will I try to alter the settings.
- using the school system or devices for online gambling, online gaming or internet shopping.
- using technologies for any illegal activities including violating copyright laws, impersonating the identity of others, forgery or other contracts.
- using other users' passwords
- trespassing in others' folders, work or files
- plagiarism (copying) of other peoples work
- employing the network for commercial purposes or activities by for-profit institutions or organisations, product advertisement or political lobbying is prohibited
- sending spam or chain letters, or other mass unsolicited mailings
- using the network to disrupt its use by other individuals or by connecting networks
- disrespect of others' privacy and intellectual property
- using staff computers, staff laptops or staff iPads.

### Guidelines

- SHSG will monitor user data, internet access and email by use of Impero which is a key logger.

- Curriculum use of the network and computer resources takes precedence over non-curriculum use.
- This statement covers (but is not limited to) the use of electronic devices owned by the school and by students that are brought onto school premises, or on excursions, camps or other official school functions including computers, laptops, storage devices, digital video and music players, cameras, other recording devices, mobile phones, iPads and organisers
- It is understood that the school is not liable for any loss or damage of personal IT devices bought into school
- It is understood that IT Support department will not repair or install any software onto personal IT devices
- Personal IT devices should use the guest wifi network only
- The school will try their best to help students join their personal devices to the guest network, but not all devices will be successful.
- Any personal laptop chargers must be taken to the IT Support office to be PAT tested (electrical safety test) before being used in school
- The student should have a working anti-virus solution on their own devices before joining the school network and is responsible for regularly running the anti-virus software.
- SHSG reserves the right to ensure all student computers and laptops have sufficient space to support learning activities. This may include the school deleting non-essential games, music and video files.
- Any damage or faults involving school equipment or software should be reported immediately however this may have happened
- ICT Rooms can be used only at lunchtimes and only for school work. The library is available at before school, break, lunchtimes and after school.
- Students who borrow a school device must sign a form saying they are responsible for the cost of any loss or damage to that device.
- Any device borrowed by the student must return it when requested or when they leave SHSG.

### **Sanctions**

- sanctions for violations involved with breaches of the acceptable use statement are listed below.

Sanctions may include the following measures:

- withdrawal of privileges including on-line access for breaches of online policy.
- withdrawal of the right to bring or use electronic devices to the SHSG or to school activities.
- payment for cost of repairs

## **For serious breaches of rules**

- suspension or expulsion
- law enforcement agencies may be involved

## **Appendix 1:**

### **Email Policy**

#### **General Information**

##### **1. The Email Service**

The email service is provided to all students of SHSG for communication purposes both within school and to email work between school and home. This is a privilege that SHSG extends to its students. This privilege will be withdrawn when the students finish their studies at SHSG. Students must observe all the rules governing student email service; otherwise, the privilege will be withdrawn.

1.2 Students will access their email via Office365. A shortcut is in the start menu at school. At home enter the school website [www.shsg.org](http://www.shsg.org) into a web browser, select student, then Office365.

1.3 The student's email login has the same username (with @shsg.org) and password as their computer network login.

1.4 The student, upon leaving SHSG, will give a personal email address for future contact. The student's school email account will be deleted one year after the student has left the school.

1.5 Student school emails should be used for educational purposes only and not for social communication.

##### **2 Rules:**

All students using the SHSG email service are required to observe the following rules:

1. Within school, students should use only their SHSG email.
2. For security, no password should be written down or stored on the network. Students should not give their password to any other person for any purpose, nor allow another student to use their email account.
3. Students shall not send inappropriate or irrelevant email to other students or a large group of recipients as it will not only waste the recipients' time and their own mailbox quota but also interfere with the normal operation of servers and networks. Typical emails considered as inappropriate are:  
Advertisements; lost and found; announcements to people you do not know; forwarding of jokes; and social emailing during lessons (email used to chat to friends). Unsolicited massive emailing is prohibited.

4. Generation or propagation of chain mail is strictly prohibited. Chain mail is equivalent to a chain letter, requesting recipients to duplicate junk mail to others, thus generating a chain of emails.
5. Students shall not send email in the name of any other person (fake mail) and shall not use anonymous mail as it is considered as an act of dishonesty. Any fake or anonymous mail may result in disciplinary action.
6. Email should always be written in formal language and observe common courtesy. Students should address teachers as they would in the classroom, and begin emails with Dear (teacher's name). Text language is not appropriate. Students should not use bad language or harass the recipient. Any indecent email is strictly prohibited.
7. Email attachments should not be bigger than 10mb in order to maintain a fast and effective service.
- 7a. Emails that are unknown or unexpected containing attachments or hyperlinks should not be opened, the hyperlinks should not be clicked into nor attachments opened as they could contain viruses or other harmful programmes. These emails should be right clicked, send to junk and block the sender.
8. The Laws of the UK governing pornographic and indecent material also apply to files stored in electronic forms. Illegal storage and distribution of such material is a criminal offence. All files sent should be copyright free, or the student must be the copyright holder. Students should also adhere to the Data Protection Act 2018 also known as GDPR.
9. A breach of any of these rules may result in suspension or removal of access privilege to the SHSG email.
10. The ICT Manager has access to all students' emails and has the authority to issue warnings to students who have breached any of these rules and to deal with the case according to school guidelines.
11. A serious breach of these rules by students will result in disciplinary action.