STEPHEN HAWKING SCHOOL
POLICY

e-Safety Policy

Document Control		
Date of Draft:	08.02.2023	
Draft Author:	Kirsty Tucker (Senior Assistant Headteacher)	
Draft Approved By:	Jennie Bird (Executive Headteacher)	
Final Approval:	21.02.2023	Governors (Resources)
	Tara Haroon (Chair of Resources)	
Policy Type:	School (Voluntary)	
Publication:	All	
Review Date:	Review Date	
Review Cycle	Biennial	

e-Safety Policy

Introduction

This e-Safety policy has built on The London Grid for Learning (LGfL) exemplar policy and other example policies and documents.

This Policy document was drawn up to protect all parties: pupils, staff and the school, and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Legal Requirements

It is the duty of the school to ensure that every child in our care is safe. The same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

Aims & Objectives

The school aims to create a safe IT learning environment which includes:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive e-safety education programme for pupils, staff and parents

Implementation

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Heads of School, with the support of governors, aim to embed safe practices into the culture of the school.

School Management Team

The SMT ensures that this policy is implemented and that compliance with the policy is monitored. The school will include e-Safety in the curriculum, where appropriate, to ensure that every pupil has been educated about safe and responsible use in line with their ability.

TLR Team & Senior Assistant Headteacher

Monitoring e-Safety is the responsibility of class teachers under the guidance of the TLR Team & the Senior Assistant Headteacher. The TLR Team & the Senior Assistant Headteacher ensure the Heads of School, senior management and governors are updated as necessary.

Governors

Governors need to have an overview understanding of e-Safety issues and strategies at Stephen Hawking School. The TLR Team & the Senior Assistant Headteacher will ensure governors are aware of local and national guidance on e-Safety and are updated as necessary.

Pupils

It is recognised that Stephen Hawking School pupils will not have the cognitive ability to have an effective understanding of e-Safety. It is important, therefore, that staff take the lead in ensuring that all pupils are safe and inappropriate sites, for example, are not accessed.

Volunteers & Visitors

Volunteers and visitors are:

- *given the school's Health and Safety and Safeguarding Information for Visitors booklet on arrival. The booklet contains basic e-Safety information.*
- *not permitted to use personal devices in the presence of pupils or to use them to photograph, video or otherwise record pupils.*
- *required to provide their organisations own consent forms for parents/carers if they wish to photograph, video or otherwise record pupils using their organisation's devices.*
- *are permitted to access the school's guest Wi-Fi, which is more restrictive than the school's standard Wi-Fi and automatically disconnects at the end of each visit.*
- *not normally given access to the school network.*

School Staff

All staff are responsible for promoting and supporting safe behaviours in their classrooms and for following the school's e-Safety procedures.

All staff should be mindful of:

- *safe use of email;*
- *safe use of the internet including use of internet-based communication services, such as instant messaging and social networks;*
- *safe use of video conferencing/remote learning apps;*
- *safe use of the school network, IT equipment and data;*
- *safe use of digital images and associated digital technologies, such as mobile phones, tablets, smart devices and digital cameras;*
- *publication of pupil information/photographs and use of the school website;*
- *PREVENT and e-bullying/cyberbullying procedures;*
- *GDPR;*
- *the school's staff code of conduct, remote learning and remote working protocols;*

- *their role in providing e-Safety education for pupils.*

Staff are reminded/updated about e-Safety matters when necessary and training, appropriate to their needs and abilities, provided as necessary.

School Internet Provision

The school uses the standard LA Internet Service Provider, which is Virgin Media Business, as part of the London Grid for Learning Broadband consortium.

Virgin provides an always-on broadband connection at speeds of up to 200 MB.

Stephen Hawking School understands that the internet is a valuable resource for school staff.

Stephen Hawking School is committed to encouraging and supporting school staff to make the best use of the internet and all the opportunities it offers to enhance teaching and support learning.

To enable staff to make full use of these important resources, the internet is available in school to all staff for professional use. The school also provides an LGfL user account that gives further access to specific resources and online tools.

Staff are expected to model appropriate IT and internet use at all times. This supports our commitment to encouraging safe and appropriate IT and internet use by our pupils both in school and at home.

Staff must also consider inclusion and equalities issues when using IT and the internet and to provide pupils, such as those with visual impairments, multi-sensory impairments or limited physical mobility, with appropriate models to support the school's Inclusion and Equal Opportunities policies.

Staff who need support or INSET in using IT as part of their professional practice can ask for support from their class teacher, the TLR team or the Senior Assistant Headteacher.

Staff are welcome to use the school internet connection for personal purposes provided that such use does not interfere with their professional duties and is in line with the school's code of conduct and terms of employment.

Network Access

The school provides all permanent staff with a log in and password allowing them to access all or part of the school network.

Staff are responsible for remembering and safeguarding their network password and ensuring that it is not shared with other staff either inadvertently or deliberately. Staff are regularly reminded of this responsibility. In line with GDPR legislation, the IT/Media Technician and the Executive Headteacher no longer have access to the passwords of existing staff via LGfL Support.

Using the log in credentials of another member of staff or using any other method of circumventing network security is forbidden.

Staff should follow the existing network file structure, conventions and restrictions when storing files and should follow the maxim of 'maximum availability' of information whenever it is safe and practicable to do so. If staff have queries or concerns about the

network file structure, they should raise them with the TLR Team or the Senior Assistant Headteacher.

Pupils are not normally provided with network access.

Email

Staff use email to communicate with other staff, with parents/carers and with external colleagues, and are provided with log in credentials to do so. Staff are responsible for remembering and safeguarding their email password and ensuring that it is not shared with other staff either inadvertently or deliberately. Staff are regularly reminded of this responsibility. In line with GDPR legislation, the IT/Media Technician and the Executive Headteacher no longer have access to the passwords of existing staff via LGfL Support.

Using the email credentials of another member of staff is forbidden.

All staff should be mindful of the need to ensure that emails are spell-checked, grammatically correct, polite and accurate at all times.

Staff are reminded that using their school email address means that they are representing the school and all communications must reflect this.

Encrypted email must be used to send sensitive information (such as pupil details) outside the LGfL mail system.

Pupils do not have access to email.

School ICT Equipment & Resources

The school offers staff and pupils access to appropriate IT equipment and resources, including computers, laptops, tablets, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.

Staff are welcome to borrow school IT equipment for home working or personal use (either in or out of school). Advance permission must be obtained from a member of the School Management Team and the loan logged by the IT/Media Technician. Staff are responsible for the equipment while it is on personal loan and may be required to reimburse the school for its loss or any damage.

School IT equipment may, on occasion, be loaned to parents/carers. This must be agreed in advance with a member of the Senior Management Team and a consent form completed by the parents/carers.

Personal Devices and Accounts

Personal devices and accounts (e.g.: personal email addresses, personal social media and instant messaging accounts etc.) may not be used for school business (with the exception of remote working), including, for example: emailing, contacting parents/carers and remote learning.

Personal devices, including mobile phones, smart watches, tablets, digital cameras and other internet enabled or smart devices, may not be used in the direct presence of pupils.

Access to the internet via the school's network for personal devices is at the discretion of the Heads of School and may be withdrawn at any time. Passwords to the school's staff Wi-Fi will not be given to staff but must be entered directly by the IT/Media Technician or the school receptionists. Staff should delete the school's Wi-Fi network from their personal device on terminating their employment with the school.

Remote Learning

Staff should follow the school's Remote Learning Staff Handbook at all times.

Parent/Carer permission must be obtained before the remote learning sessions begin for each pupil.

A second member of staff (preferably from the same class team) must be present online or in person for the entirety of any remote learning session.

Staff should follow safe practice and the most recent local authority and Government guidance when using remote learning software, including regularly changing personal IDs and passcodes, locking sessions once underway etc. If an uninvited person enters a remote learning session, the session should be ended and the Designated Safeguarding Lead informed as soon as possible.

Remote Working

Staff may request to or be requested to work from home in special circumstances.

Remote access to the school network and/or a school device may be provided to staff upon request and with the agreement of a member of the Senior Management Team to support remote working. School devices may only be used for school purposes and staff should not install their own software/apps on them. Staff should not store sensitive school information on the local drive of their school device for any longer than absolutely necessary. The school may request the return of the device, temporarily or permanently at any time. The IT/Media Technician may request evidence that the device is still in the possession of the loanee at any time. All teaching staff are provided with an encrypted USB device for the transfer of sensitive information.

Staff are permitted to use their personal device for remote working provided that they have confirmed that the device has appropriate and up to date anti-virus/anti-malware measures installed on it. Staff are not permitted to store sensitive school information on their personal device for any longer than absolutely necessary. Whilst using their personal device, staff must still adhere to the school's code of conduct and not use personal email/social media to conduct school business.

The school does not undertake to provide an internet connection for staff remote working nor to reimburse staff for the cost of their internet connection while remote working.

Content Filtering

The LGfL uses a sophisticated content filter to ensure that, as far as possible, only 'appropriate' content from the Internet finds its way into school. Whilst this filtering

technology is robust and generally effective at blocking 'inappropriate' material, it is still possible for 'inappropriate' material to occasionally get past the filter. If this happens:

- *Staff must inform the appropriate Head of School, the Designated Safeguarding lead and the IT/Media Technician. Parents/carers will be informed where necessary.*
- *Staff who deliberately use school IT equipment or resources to try to access material deemed 'inappropriate' by the school, or use their own equipment or resources to share such material with pupils will be dealt with according to the school's code of conduct and conditions of employment.*

Downloading Files and Applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed.

- *Although LGFL content filtering is in place, staff are advised to exercise caution when downloading material and should consult the IT/Media Technician before installing any applications or software.*

Portable Storage Media

Portable storage media such as USB flash drives are a common way of introducing a virus or other undesirable agent onto a school computer system.

- *Staff will only use portable storage media supplied by school or agreed by the IT/Media Technician if absolutely necessary.*
- *Encrypted portable storage media must be used when transporting sensitive pupil information or software.*

Virus & Malware Protection

The school's anti-virus/anti-malware software is monitored and updated regularly by LGfL and the IT/Media Technician.

- *Any software messages or pop-up screens reporting evidence of viral/malware infection should always be reported immediately to the IT/Media Technician.*

Use of the Internet by Pupils

Internet access is carefully controlled by the class teacher (or the class STA in the teacher's absence) according to the age and experience of the pupils and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the internet. With iPads now in use in the classroom, staff constantly monitor the online activities of students.

'Inappropriate' Material

Despite the best efforts of the LGfL and school staff, staff and/or pupils may occasionally come across something on the internet that they find offensive, inappropriate, unpleasant or distressing.

Staff should always report such incidents directly to the TLR Team & the Senior Assistant Headteacher and to the IT/Media Technician at the time they occur, so

that action can be taken. The action will include:

- *logging the incident and making a note of the website and any other websites linked to it;*
- *informing the appropriate Head of School and the Designated Safeguarding Lead;*
- *informing the LA/Internet Service Provider so that the website can, if necessary, be added to the content filter if the IT/Media Technician is unable to do so.*

Staff should remember that their personal view of what constitutes offensive, inappropriate, unpleasant or distressing, may not be shared by other staff or the school.

School Website

The school website is the public face of the school. Resources intended for the website must be spell-checked, grammatically correct, copyright compliant, polite and accurate at all times and it is the responsibility of the member of staff providing them for upload to ensure this.

Resources for use with pupils should be appropriate to the needs of the pupils for whom they are intended.

Copyrighted material cannot be hosted on the school website.

Photos and videos for upload to the website should be carefully checked by the creator for any sensitive material that may be visible in the background and any such material removed or hidden before submission.

Parents/Carers must consent to their child(ren)'s image(s) being used on the website in either photos or videos.

It is the responsibility of a pupil's class teacher or most recent class teacher to inform the IT/Media Technician as soon as possible if a child whose image appears on the website is deceased, has left the school or whose image can no longer feature. The child's image will then be removed as soon as possible.

Errors in the school website should be brought to the attention of the IT/Media Technician. Changes to the website should be discussed with the TLR team/Senior Assistant Headteacher in the first instance.

Instant Messaging, Forums and Social Networking

Staff should not access instant messaging or social networking sites or apps in the direct presence of pupils.

Pupils' personal details, identifying information, images or other sensitive details may never be used for any public internet-based, instant messaging or social networking activity unless written permission has been obtained from a parent/carer.

Staff should not discuss pupils or school business on their personal instant messaging or social networking accounts or engage with others who may have done so. Any such discussion should be bought to the attention of the appropriate Head of School as soon as possible.

Staff may not 'friend' parents/carers of current pupils via their personal instant

messaging or social networking accounts.

Assessment

E-safety is recognised as an essential aspect of strategic leadership in this school and the Heads of School, with the support of governors, aim to embed safe practices into the culture of the school.