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, in particular the policy from Clara Grant School.

This policy document is 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/carers.

Implementation

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

Leadership Team

The School Management Team 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.

IT Co-ordinators

The school will monitor e-safety. It will be the responsibility of class teachers under the guidance of the IT co-ordinators. The school's IT co-ordinators ensure the Senior Management Team 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 IT co-ordinators will ensure governors are aware of local and national guidance on e-safety and are updated as necessary.

School Staff

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

All staff should be mindful of:

- safe use of e-mail and the Autotext system;
- safe use of internet including use of internet-based communication services, such as instant messaging and social networks;
- safe use of the school network, IT equipment and data;
- safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of the school website;
- safeguarding, e-bullying and cyberbullying procedures;
- GDPR
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety matters when necessary.

Pupils

It is recognised that the 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.

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 up to 100 MB.

Content filtering

The LGfL use 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.

- All pupils and staff must inform the Senior Management Team and the IT/Media Technician if this happens. 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 rules outlined elsewhere in this document.

Downloading Files & Applications

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

- Although LGFL internet filters are 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.
- Encrypted portable storage media must be used when transporting sensitive pupil information.
- Staff are responsible for checking that effective anti-virus software is installed on any non-school provided equipment before attaching school provided portable storage media to it.

Security & Virus Protection

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

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

Use of the Internet by Pupils

Internet access is carefully controlled by teachers 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 in use in the classroom, staff need to be constantly monitoring the online activities of students.

'Inappropriate' Material

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

Staff are told to always report such experiences directly to the IT co-ordinators and 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 Senior Management Team;
- informing the LA/Internet Service Provider so that the website can, if necessary, be added to the content filter.

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.

Using Email at School

Pupils do not have access to email.

Staff use email to communicate with other staff, with parents/carers and with external colleagues. All staff should be mindful of the need to ensure that emails are polite and accurate at all times.

Staff should use USO/FX, Proton Mail or other secure systems when emailing sensitive information to users outside LGfL.

Instant Messaging, Forums & Social Networking

Staff should not access instant messaging or social networking sites or apps in the 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 media activity unless written permission has been obtained from a parent/carer.

Assessment

None

Review

This policy will be reviewed every two years.

Appendix I: Use of the Internet and ICT Resources by School Staff

The Internet

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

We are 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.

Internet Availability

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.

IT Equipment & Resources

The school also 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.

Professional use

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 with appropriate models to support the school 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 the IT Co-ordinators.

Personal Use of the Internet & IT resources

We recognise that staff may occasionally find it useful to use the internet at work for personal purposes. They may also wish to borrow school IT equipment for personal use, either in or out of school.

Some equipment is available for loan to staff, with permission from the IT/Media Technician and/or the Senior Management Team. The loan must be logged.

All staff must, however, be aware of the school policy on using the school internet and IT resources for personal use. These are outlined in the staff agreement form below.

Email & Autotext

We recognise that email is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school email address and we ask staff to use it, or other agreed secure electronic communication, for all professional communication with parents/carers, colleagues, external organisations, companies and other groups.

Personal email addresses and personal devices must not be used for school/professional communication.

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

Staff should use USO/FX, Proton Mail or other secure systems when emailing sensitive information to users outside LGfL.

Staff may only text parents/carers via the school's Autotext system.

Instant messaging, forums and social networking

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

When accessing instant messaging, forums and social networking using the school's internet or IT resources, staff should apply professional standards to all postings and messages.

Access to the school's internet for BYO (Bring Your Own) devices where agreed may be withdrawn at any time at the Senior Management Team's discretion.

Data Protection and Copyright

The school has a Data Protection Policy in place – please see separate documentation for more details.

Staff are aware of this policy and how it relates to Internet and IT use, in particular with regard to pupil data and photographs and follow the guidelines as necessary.

Staff should understand that there are complex copyright issues around many online resources and materials and must always give appropriate credit when using online materials or resources in teaching and learning materials.

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

We adhere to the LA Guidelines on Data Protection.

Staff understand the legal and disciplinary implications of using the internet at school for illegal purposes and monitor pupils with this in mind.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the internet by members of the school community using the connection provided by the school.

1. School Staff Agreement Form

This document covers the use of school digital technologies and networks in and out of school.

Access

- I will obtain the appropriate log on details and passwords from the IT/Media Technician
- I will not reveal my password(s) to anyone other than the person responsible for managing the network.
- If my password is compromised, I will ensure I have it changed.
- I will not use anyone else's password if they reveal it to me.
- I will not allow unauthorised individuals to access school IT systems or resources.

Appropriate Use

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking identities/blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure that my activities on social media do not breach professional conduct standards.
- I will never include pupils as part of a non-professional social network or group and will exercise careful judgment when including adult former pupils.
- I will ensure that I represent the school in a professional and appropriate way when sending email or texts, contributing to online discussion or posting to public websites using school facilities.
- I will not use school IT equipment or resources to try to access material deemed 'inappropriate' by the school, or use my own equipment or resources to share such material with pupils.
- I will report any accidental in school access to, or receipt of, 'inappropriate' materials, or filtering breach to the Senior Management Team and the IT/Media Technician.

Professional Conduct

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites/blogs etc that I create or actively contribute to are not confused with my professional role.
- I will never include pupils and parents/carers as part of a non-professional social network or group. I will exercise careful judgment when including adult former pupils.
- I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities.
- I will not use my personal device for school business.

Email

- I will only use my LGfL email or other agreed email system for school business or communication with parents/carers.

Photographs and Video

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff or store pupil images at home without permission from the Senior Management Team.
- I will show vigilance when short term supply staff are on site and report anything I feel is potentially against school policy to the Senior Management Team. I will ensure that any visitors for whom I am responsible have read the school's Health & Safety and Safeguarding Information for Visitors leaflet.

- I will never associate pupil names or personal information with images or videos published in school publications or on the internet (in accordance with school policy and parental guidance) without written permission from the Senior Management Team.

Personal Use

- I understand that I may use Internet facilities for personal use at lunchtimes, break times and before and after school, where computers are available and not being used for educational purposes.
- I will not access instant messaging, social networking sites or apps or personal email in the presence of pupils. I will not download any attachments, pictures or other material from these onto school computers or the school network.
- When accessing instant messaging, forums and social networking using the school's internet or IT resources, I will apply professional standards to all postings and messages.
- I understand that access to the school's internet for BYO (Bring Your Own) devices where agreed may be withdrawn at any time at the Senior Management Team's discretion.

Use of School IT Equipment out of school

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any 'significant personal use' as defined by HM Revenue and Customs.
- I will keep any loaned IT equipment up-to-date, including updating the provided anti-virus software and installing Windows updates as required.
- I agree to return any loaned IT equipment to school or provide appropriate evidence of its continued use when requested to do so by the IT/Media Technician.
- I will remove any software or apps that I have installed on school IT equipment before returning it. I will also remove all personal or school data.
- I will not connect a computer, laptop or other device to the network that does not have up-to- date anti-virus software. I will inform the IT/Media technician before connecting my device or that belonging to any visitor for whom I am responsible.

Teaching and Learning

- I will always actively supervise, or arrange for suitable adult supervision of, pupils that I have directed or allowed to use the internet.
- I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials.
- I will ensure I am aware of digital safeguarding issues so they are appropriately embedded in my classroom practice.

Copyright

- I will not publish or distribute work that is protected by copyright.
- I will reference online resources when I use them in a report or publication.

Data protection

- I will not give out or share personal addresses (including email) or telephone/fax numbers of any member of staff without permission from the Senior Management Team.
- I will not take pupil data, photographs or video from the school premises without the full permission of the Senior Management Team.
- I will ensure any confidential data that I wish to transport from one location to another is

protected by encryption and that I follow school data security protocols when using any such data at any location.

- I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

E-Safety Policy, Staff Agreement

Form User Signature

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I wish to have an email account, be connected to the internet via the school network and be able to use the school's IT resources and systems.

Signature ..... Date .....

Full Name .....(printed)

Job title .....

School .....

Authorised Signature (Senior Management Team)

Signature ..... Date.....