E-safety Policy

Member of staff responsible: Harley Greer
Date agreed by GB: May 2024
Date to be reviewed: Summer term 2026

Contents of E-safety Policy:

1. Introduction

At South Harringay, we recognise the contribution of online services towards raising educational standards, promoting pupil achievement, and enhancing teaching and learning. Hence, the use of online services is embedded throughout the school; consequently, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. It has been agreed by the senior leadership team and approved by Governors. It will continue to be reviewed annually.

2. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Whistleblowing Policy
- Technology Acceptable Use Agreement: Pupil and Adults (E-safety policy)
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Positive Relationship Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Use of Digital Images
- Staff IT Equipment Loans
- Remote Education Policy

3. Roles and Responsibilities

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

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the E-safety Policy.

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL and Computing lead's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with the school's IT providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges.

Headteacher

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the IT technicians to conduct **termly** light-touch reviews of this policy.
- Working with the governing board to update this policy on an **annual** basis.

Leadership team

The Senior Leadership Team (SLT) ensures that the policy is implemented across the school via the usual school monitoring procedures.

SLT will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and IT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

E-safety Coordinator

Our school Computing and Digital Literacy lead, Harley Greer, is responsible for keeping up to date on all E-safety issues and ensuring that staff are updated as necessary.

The E-safety coordinator will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and IT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring all members of the school community understand the procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Working with the IT technicians to understand the filtering and monitoring processes in place at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Working with the headteacher and IT technicians to conduct **termly** light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an **annual** basis.

IT technicians

Our IT technical team, Crossover Solutions, and school technician, Aman Basra, will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the headteacher, SLT and E-safety coordinator to conduct **termly** light-touch reviews of this policy.

School Staff

All school staff are responsible for:

- Promoting and supporting safe behaviours through following school E-safety procedures in both their physical and virtual classrooms. This includes fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.
- Ensuring they are familiar with the school E-safety policy, and must ask for clarification where needed.
- Signing the Staff Acceptable Internet Use agreement annually.
- Class teachers must ensure that pupils are aware of the E-safety rules, which must be introduced at the beginning of each new school year.
- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.

Pupils

Pupils are responsible for:

- Taking an active part in planned lessons and activities to support their understanding and confidence in dealing with E-safety issues.
- Signing the Pupil Acceptable Use Agreement at the beginning of each academic year that outlines the guidelines and rules covering their responsibilities when using IT at school.

Parents

Parents are given information about the school's E-safety policy at the admission interview. They are given copies of the Pupil's Acceptable Use Agreement for information, and asked to support these rules with their children.

4. Technical and hardware guidance

School Internet provision

The school uses the standard LA Internet Service Provider, which is the London Grid for Learning Broadband consortium.
They provide an always-on broadband connection at speeds up to 200 MB.

Content filter

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 unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- *All pupils and staff have been issued with clear guidelines on what to do if this happens, and parent will be informed where necessary.*
- *Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document and in line with the school Positive Relationship policy in the case of children and the Disciplinary policy in the case of staff.*

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 on a computer. Whilst some of this material may be useful,

much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- *Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.*

Portable storage media

- *Staff are allowed to use their own portable media storage (USB Keys etc) after it has been scanned. If use of such a device results in an anti-virus message they should remove the device and immediately report to the IT helpdesk.*

Security and virus protection

The school subscribes to the LA Antivirus software program, which uses Sophos Antivirus software.

The software is monitored and updated regularly by the school technical support staff

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

5. E-safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and IT is an integral part of that world. At our school, we are committed to teaching pupils to use the IT effectively and appropriately in all aspects of their education.

a) Internet access at school

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.

Access for all pupils

In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the Internet, particularly where this will directly support their learning.

b) Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.
Using the Internet for learning is now a part of the Computing Curriculum (Sept 2014).

We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

Google Classroom and Google Meets

We recognise the need for pupils to have a secure remote learning platform for distant learning and homework. Therefore, as a school, we use the Google Classroom platform. Teachers are given clear direction on remote learning through the Remote Learning Policy. All children have their own personal usernames and passwords to access Google Classroom. Children are consistently reminded not to share their personal login details. Teachers are able to create secure live sessions with pupils via Google Meets. In order to promote secure access, the link to Google Meets is only shared within the pupil's Google Classroom five minutes before a session goes live.
Members of the SLT consistently monitor each virtual classroom to ensure that it is being used by staff and pupils as outlined in the Remote Learning Policy.

c) Teaching safe use of the Internet

We understand that our pupils are growing up with technology at their fingertips; hence we believe that a secure awareness and understanding of E-safety is of great importance. Therefore, E-safety is taught as part of the Computing curriculum as well as an independent subject in its own right.

E-safety is integrated wherever relevant within our day-to-day practice and concise, cross-curricular links are made with all subjects to enhance knowledge. Children are exposed to an E-safety programme throughout their time in our school: providing access to age-appropriate messages and content that supports them to: use technology safely, respectfully and responsibly; recognise acceptable and unacceptable online behaviours; and identify where to seek advice and help should they have any concerns about their online experiences.

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area:

Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
http://www.kidsmart.org.uk

The main aspects of this approach include the following five **SMART** tips:

- **Safe** - Staying safe involves being careful and not giving out your name, address, mobile phone number, school name or password to people online. Remember personal information can be seen in images and videos you share too, keep them safe to keep yourself safe.
- **Meeting** someone you meet in cyberspace can be dangerous. If someone you only know online ever asks you to meet up or for personal information then tell a trusted adult.
- **Accepting** – Think carefully before you click on or open something online (e.g links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. If you are unsure who it is from or what it is, do not accept it.
- **Reliable** – You cannot trust everything you see online as it could be out of date, inaccurate or not entirely true. To find reliable information you should check at least three different websites, check in books and talk to someone about what you have found.
- **Tell** a trusted adult if someone or something makes you feel upset, worried or confused.

Suitable material
We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Non-Education materials
We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, outside of school and at home.

Unsuitable material
Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the E-safety coordinator
3. Logging the incident on My Concern
4. Logging the incident – IT helpdesk

5. Discussion with the pupil about the incident, and how to avoid similar experiences in future
6. Inform the parents of the child

For more information on unsuitable material and over-use see SHS 'What do we do if …' guidance page 20

d) Using E-Mail at school

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively. Through our Computing curriculum, pupils are taught how to safely use email through the online platform Purple Mash. This programme allows pupils to send and receive emails during Computing lessons, and this is monitored closely by staff. Teachers are responsible for restricting the use of email outside of lesson time and outside of school via the settings within Purple Mash.

- Pupils are not allowed to access personal e-mail accounts using school Internet facilities

e) Chat, discussion and social networking sites

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

We use the resources, guidelines and materials offered by Kidsmart, as outlined above in the Safe use of the Internet section to teach children how to use chat rooms safely.

All commercial Instant Messaging and Social Networking sites are filtered as part of the LA Internet policy.

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

f) Other online technologies

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

- Pupils are not allowed to have personal mobile phones or other similar devices in school. If parents request children to carry a mobile phone, such devices will be kept in the class room by the class teacher for pupils who may need them on their journey to and from school.

g) Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- Complaints of cyber-bullying are dealt with in accordance with our **Anti-Bullying Policy.**
- Complaints related to child protection are dealt with in accordance with safeguarding procedures.

h) Contact details and privacy

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.
Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet. (section 5c)

School and pupil websites – pictures and pupil input

As part of the IT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform.

Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images restricted.

j) Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should be displayed in each classroom.
Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse in accordance with the school's Positive Relationship policy.

Sanctions will include:

Unsuitable material (e.g., online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from class teacher
- Loss of playtime
- Report to Headteacher
- Letter to parent/carer

Offensive material (e.g., pornographic images, racist, sexist or hate website or images etc)

- Initial letter to parent/carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer to re-sign Internet use agreement
- Loss of playtime
- Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

j) Complaints

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.
International scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.
Sanctions available include:

- All incidents will be recorded

- Interview/counselling by class teacher, SLT, E-safety Coordinator and Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period,
- Referral to LA / Police.

Any complaint about staff misuse is referred to the Head teacher.

k)

Pupil Acceptable Use Agreement

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

1. I will ask permission before using any IT equipment (e.g., computers, digital cameras, etc), and only use it when a teacher or another adult is with me.
2. I will only use the school's computers for schoolwork and homework.
3. I will only delete my own files, and I will not look at other people's files without their permission.
4. I will use the usernames and passwords provided by the school to access the school network.
5. I will not bring software or USB memory sticks into school without permission.
6. I will ask permission before using the Internet, and only use it when a staff member is present.
7. I will only visit web sites that I am asked to by school staff, or that have been saved in a shared internet link folder for pupils to use.
8. I will not use Google image search without being asked to do so by a school staff member.
9. I will not download anything (files, images etc) from the Internet unless given permission.
10. I will only use an approved email account provided for me by the school to send email as part of my learning. I will not use personal email accounts (e.g. Hotmail) at school.
11. The messages I send or information I upload as part of my school work will always be polite.
12. I will not use my full name, give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family or my friends, unless my teacher has given permission.
13. If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it but I will immediately tell a school staff member.
14. I will use the Kidsmart website to help me understand how to keep safe when using ICT.
15. I understand that the school may check my computer files, e-mail and the Internet sites I visit, to help keep me safe.
16. I understand that if I deliberately break these rules my parents and the Headteacher will be informed.

6. Use of the Internet and IT resources by school staff

The Internet

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our 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, online tools and email.

IT Equipment and Resources

The school also offers staff access to appropriate IT equipment and resources, including computers, laptops, iPads, interactive whiteboards, data projectors, digital cameras, video 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 are also careful to 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 that need support or additional training in using IT as part of their professional practice can ask for support from the Computing subject lead.

Personal use of the Internet and IT resources

Some equipment may be available for loan to staff, with permission from the subject lead. However, all staff must be aware of the school policy on using school Internet and IT resources for personal use. These are outlined in the staff agreement form below.

E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat and messaging

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums to share good practice and disseminate information and resources.

The use of online discussion groups relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

Social Networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and the SHS E-safety policy staff agreement form (section 7).

Data Protection and Copyright

The school has a data protection policy in place – please see section 8

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 understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

7. Staff Acceptable Use Agreement form

SHS E-safety Policy Staff Agreement Form

This document covers use of school digital technologies, networks etc both in school and out of school.

Access

• I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
• If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
• I will not allow unauthorised individuals to access school IT systems or resources.

Appropriate Use

• I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
• I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
• I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network.
• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the E-Safety coordinator or member of the SLT.

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 or former pupils as part of a non-professional social network or group.
• 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 browse, download or send material that could be considered offensive to colleagues.
• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the E-Safety coordinator or member of the SLT.

Personal Use

• I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
• I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
• I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
• I will not use the school Internet facilities for personal access to public discussion groups or social networking sites.

Email

• I will only use the approved, secure email system for any school business: (currently: LGfL Mail)
• I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

Use of School equipment out of school

• I agree and accept that any equipment loaned to me by the school, is provided mainly 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 not connect a personal laptop or other device (including USB flash drive) that was used at home to the school network / Internet if it does not have up-to-date anti-virus software and has been scanned.

Teaching and Learning

• I will always actively supervise, or arrange for suitable 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.
• I will only use the Internet for professional purposes when pupils are present in the classroom.

Photographs and Video

• I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home.
• 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).

Data protection

• I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.
• I will not take pupil data, photographs or video from the school premises e.g., on a memory stick or any other removable media.
• I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises.
• 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, will 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.

Copyright

• I will not publish or distribute work that is protected by copyright.
• I will encourage pupils to reference online resources and websites when they use them in a report or publication.

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 agree to have a school user 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 .....

8. Data Protection Policy

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

The school holds information about children and adults and we process it in a number of ways to improve the quality and standard of our provision. If information needs to be passed on electronically then files must be encrypted before they are sent. If an organisation wants to obtain sensitive or confidential information about any pupil, then consent from the pupil's parents must be sought.

We adhere to the LA Guidelines on Data protection.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

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.

9. IT Equipment Loans

Staff Loans

Any member of staff who borrows or uses any IT equipment must adhere to all aspects of this E-safety Policy.

This must be the case wherever an iPad, camera or other such device is being used as it remains the property of South Harringay School at all times.

Staff must take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to

exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Pupil Loans

The school will loan certain pieces of IT equipment to support children in remote learning, in certain situations; for example, during Pandemic lockdowns or if a child is at home for an extended period due to illness or injury.

All items loaned to pupils must be checked before they are loaned out, to ensure they do not have any sensitive information stored on them, which could contravene our GDPR legislation.

The parent/carer of the pupil is responsible for the acceptable use of the equipment while it as at home, as well as the safe return of the equipment to school at the end of the loan period. The parent/carer must sign a loan agreement before the equipment is taken home.

All equipment must be checked by one of our IT consultants on its return to ensure that it is working properly, and that there is no evidence of any improper usage. Any improper usage must be reported to the DSL immediately, so that any safeguarding issues can be assessed and dealt with promptly.

10. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.
The DSL has overall responsibility for the school's approach to online safety, with support from the E-safety lead and SLT, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular safeguarding training that incorporates online safety
- Staff are informed of any changes to online safety guidance or legislation by the E-safety lead
- E-safety lessons are conducted half-termly on the topic of remaining safe online
- Online safety is integrated into learning throughout the curriculum

a) Handling online safety concerns

Any disclosures made by pupils to staff members about online bullying, abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the E-safety lead and DSL, who investigates concerns with relevant staff members, e.g., the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g., the Positive Relationships Policy and Child Protection and Safeguarding Policy.
Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

All online safety incidents and the school's response are recorded by the DSL and E-safety lead.

b)

SHS 'What do we do if… '

An inappropriate website is accessed <u>unintentionally or intentionally</u> in school by a teacher or child.

1. Play the situation down; *don't make it into a drama.*
2. Make a note of the website and any other websites linked to it.
3. Report to the head teacher/ E-safety co-ordinator and decide whether to inform parents.

If incident raises a safe-guarding nature-inform DSL. Log incident in My Concern.

4. Submit incident – IT helpdesk
5. Discussion with the pupil/adult about the incident, and how to avoid similar experiences in future.
6. Inappropriate website access that is intentional will result in appropriate sanctions for the child (see Positive Relationship policy).

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the device.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the device to a secure place.
   - Instigate an audit of all IT equipment by the school's IT providers, this could include LGfL and the technical support provider to ensure there is no risk of pupils accessing inappropriate materials in the school.

- Identify the precise details of the material.
- Take appropriate disciplinary action (contact Personnel/Human Resources).
- Inform governors of the incident.

4. In an extreme case where the material is of an illegal nature:

Contact the local police or The Child Exploitation and Online Protection Command (CEOP) and follow their advice.

- If requested to remove the device to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including E-safety, Anti-bullying and PHSE, and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Notify parents of the children involved.
5. Consider delivering a parent workshop for the school community.
6. Inform the police if necessary.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA E-safety officer.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

1. Report to and discuss with the DSL in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA E-safety officer.

All of the above incidences must be reported <u>immediately</u> to the head teacher and E-safety co-ordinator Harley Greer

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

11.

E-safety agreement form: parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I am aware that my child will have access to use the Internet and other IT facilities at school.

I know that my child has signed an E-safety agreement form and that they have a copy of the 'rules for responsible IT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching E-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their E-safety or online behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's E-safety.

Parent / guardian signature: _____

Date: __/__/__

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose:

Parent / guardian signature: _____

Date: __/__/__

12.

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your child.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupil's work, we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g., photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school;
  e.g., in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g., within a document sharing good practice; in our school prospectus or on our school website. In rare events, your child could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we want your child's image linked to their name we would contact you separately for permission, e.g., if your child won a national competition and wanted to be named in local or government literature.