E-Safety Policy

Agreed:	May 2023
Review frequency:	Annually
Next scheduled review date:	May 2024

TABLE OF CONTENTS

Scope of the Policy	2
Teaching and Learning	4
Managing Internet Access	4
Policy Decisions	7
Communications Policy	7
Writing and Reviewing the E-Safety Policy	8

Our e-safety policy has been written by the school, building on best practice and government guidance. It has been agreed by the senior management team and approved by the governors.

The e-safety policy relates to other policies including those for anti –bullying and for child protection.

At our school, the e–safety coordinator works alongside the Designated Safeguarding Lead (DSL) who is the Headteacher.

Scope of the Policy

This policy applies to all members of the *school (including* staff, pupils, volunteers, parents/ carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of school.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The day to day responsibility for online safety will be delegated to the Online Safety Coordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also provides support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

Online Safety Coordinator

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

- Attends regular meetings regarding Internet Safety updates and issues.
- Reports regularly to the Senior Leadership Team.

Technical staff

The Network Manager and Technical Staff are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements set by Learning Partners Academy Trust.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- They keep up to date with Internet Safety technical information in order to effectively carry out their Internet Safety role and to inform and update others as relevant.
- That the use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the Head teacher or Online Safety Coordinator for investigation.
- That monitoring software and systems are implemented and updated as agreed in the school's policies.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the school's Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy and Agreement (AUP).
- They report any suspected misuse or problem to the Head teacher or Online Safety Coordinator for investigation.
- All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety Policy and acceptable use policies.
- They monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead:

Is trained in Online Safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal /inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils:

- Are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Understand how to be a good digital citizen and apply these skills when using digital technology
- Have a good understanding of research skills
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through drop in sessions, parents' evenings, newsletters, the school website, letters, information about national and local online safety campaigns and through Parent Online Safety Workshops. The school will include a section in the Home School Agreement relating to Internet Safety, which all parents are asked to sign at the start of Nursery and Reception. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- To support the school in encouraging good online safety practice outside of school.

Teaching and learning

Why Internet and digital communications are important

1. The Internet is an essential element in 21st century life for education, business and social interaction
2. The school has a duty to provide children with quality Internet access as part of their learning experience
3. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
4. The school Internet access is provided by Open Telecom
5. Contract and includes filtering appropriate to the age of pupils
6. Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use - **Appendix 1**
7. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
8. Pupils will be shown how to publish and present information appropriately to a wider audience

Pupils will be taught how to evaluate internet content

1. The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
2. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
3. Pupils will be taught how to report unpleasant Internet content using a tool on the Google Chromebooks and iPads

Managing Internet Access

Information system security

1. School ICT systems security will be reviewed regularly by the Safeguarding Lead and the Computing Lead
2. Virus protection will be updated regularly.
3. Headteacher receives email notifications of any internet searches and websites, which are blocked or contain unsuitable content by all login accounts using our school system (these emails are automatic and instant)
4. Regular checks are made using Securely Filtering System to monitor researches made by all staff and pupils
5. These are checked and signed by our Head teacher and logged in a secure file to monitor this data
6. Virus protection is updated regularly
7. In liaison with the Learning Partners guidelines, security strategies will be reviewed and updated as necessary

Mobile Technologies (including BYOD/BYOT)

- The school Acceptable Use Agreements for staff and parents/carers considers the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff / Governor owned**	**Visitor owned**
Allowed in school	***Yes***	***Yes***	***Yes***	***None***	***Yes***	***Yes***
Full network access	***Yes***	***Yes*** ***Pupils have restricted access**	***Yes***	***None***	***No***	***No***
Internet only				***None***	***Yes***	***No***
No network access				***None***	***No***	***No***

E-mail

- Although security software is in place, it is sensible to regard unrecognised incoming email as suspicious and attachments are not opened
- Staff to parent email communications must only take place via a school email address
- Staff to external agencies/ professionals emails must not contain any personal information e.g. a child's full name. Where necessary emails should be password protected using Egress Switch

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name - in accordance with the consent obtained from parents

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Guidance on the use of photography and video equipment is issued to parents
- Photographs that include pupils will be selected carefully and will not enable individuals to be clearly identified. The school will look to seek to use group photographs rather than full face photos of individual children
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Social networking

- Access to social networking sites for children will not be permitted in school.
- Pupils are advised never to give out personal information of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Contact between staff using email or social networking sites

- Members of staff should be aware of how their 'out of school conduct' might be portrayed or interpreted via social networking sites

Managing filtering

- The school will work in partnership with Learning Partners Academy Trust to ensure systems that protect pupils are reviewed and improved
- If staff or pupils come across unsuitable online materials, the site must be reported to the E-safety Coordinator
- Senior staff and School Business Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any incidents will be recorded in a log, these incidents will be monitored and actions will be put in place accordingly

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Staff will use a school phone where contact with pupils/carers is required
- Mobile phones and associated cameras will not be used during lessons, formal school time or in the presence of pupils at any time. The sending of abusive or inappropriate text messages is forbidden
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising internet access

- All staff must read and sign the 'Acceptable Use Policy ' before using any school electronic device or accessing emails – **Appendix 2**
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- Internet access for children will be by adult demonstration with direct supervision and access to specific, approved online materials
- Any person not directly employed by the school will be asked to sign an 'Acceptable Use Policy' before being allowed to access the internet from the school site- **Appendix 2**
- Parents will be made aware of the school's E-safety Policy is available to access on the school website

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Learning Partners Academy Trust can accept liability for the material accessed, or any consequences of Internet access
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective

Handling E-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headteacher and if the complaint is about the Head teacher, this must be referred to the Chair of Governors
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the Internet and this will be in line with the schools behaviour policy
- All staff members can log behaviour and safeguarding issues related to online safety via the CPOMS system

Community use of the Internet

All use of the school internet connection by community and other organisations shall be in accordance with the school E-safety Policy.

Communications

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety Policy will be shared with pupils
- E-safety rules will be posted in all networked rooms
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils. This will be addressed each year as students become more mature and the nature of newer risks can be identified

Staff and the E-safety policy

- All staff will be given the school E-safety Policy and its importance explained
- All staff will sign to acknowledge that they have read and understood the E--safety Policy and Acceptable Use Policy and agree to work within the guidelines – **Appendix 2**
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by the senior leadership team and have clear procedures for reporting issues
- Staff should ensure that iPads are kept secure at all times when not in use. They should not be used for social networking or personal use.

Enlisting parents support

1. Parents and carers attention will be drawn to the school E-safety Policy in newsletters and on the school website.
2. Parents and carers will be provided with additional information and guidance on E-safety via the school newsletter, E-safety pages on our school website, through ParentMail information, drop in sessions and Online Safety Workshops
3. The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school
4. Parents will be encouraged to interact with their children whilst using the internet and encourage good online safety practice

Writing and reviewing the E-safety policy

- The E-safety Policy relates to other policies including those for Computing, bullying and for child protection.
- The school has an E-safety coordinator
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership team and approved by governors

Think before you click or tap...

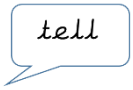
These rules help me to stay safe on a computer, tablet and iPad at school and at home:

I will always ask a grown up first before using a computer, tablet or IPad.

I will always ask a grown up first before using a Chromebook or tablet.

I will only use websites an adult has chosen and when an adult is with me.

I will only click on buttons and links when I know what they do.



I will always tell an adult if I find something that makes me feel sad or worried when I am using a Chromebook or tablet.

I know I can click on the '?' button on the Chromebooks at school if I need help.

I will not tell anyone my passwords.

I agree to follow the E-safety rules and I will be smart when using the internet at school and outside of school:
Pupil signature:

……

Class…… Date……

Appendix 2

Staff, Governor and Visitor

Acceptable Use Agreement/ICT Code of Conduct

IT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Carrington or the E-safety coordinator (Mrs Cichowska).

- I appreciate that IT includes a wide range of systems, including mobile phones, iPads, digital cameras; email, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I will only use the school's email / Internet / and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not install any hardware or software without the permission of the Head teacher
- I will ensure that personal data, such as data held on SIMS is kept secure and is used appropriately, whether in school or taken off school premises.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that children's personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head teacher.
- I understand that personal devices, such as personal cameras and smartphones will not, under any circumstance be used to take or store images of pupils.
- I understand that all my use of the Internet and other related technologies are monitored and logged and can be made available, on request, to the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will report any incidents of concern regarding children's safety to the E-safety Coordinator, the Designated Child Protection Coordinator or Headteacher and record my concern on an Expression of Concern form which will be logged.
- I will ensure that electronic communications with pupils and carers including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will support the school's E-safety policy and help pupils to be safe and responsible in their use of IT and related technologies. I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I have completed the Acceptable Usage Agreement for Tablets of Chromebooks.

User Signature

I agree to follow this code of conduct and to support the safe use of IT throughout the school. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation's most recent Acceptable Use Agreement (AUA).

Full Name …….. (print)

Job title ……..

Signature …….. Date…….

NB: This is also an electronic form

Appendix 3

Staff, and Visitor

Acceptable Use Agreement / Tablet, iPad and Chromebook Acceptable Usage Agreement

- I am responsible for the care, maintenance, charging and security of my tablet
- I am responsible for the overnight safekeeping of my tablet
- I understand I need to store my tablet in a safe place overnight (classroom cupboard out of eyesight)
- I understand that only apps authorised by the Senior Management Team or Mrs Cichowska are to be downloaded
- I understand that tablets and Chromebooks must only be used for educational purposes or to support children and adults work in school. They must not be used for personal use
- I am aware that the filtering settings are set for adults (teachers) at present. If I am using a tablet with a child for an educational purpose I must be present at **all** times
- I understand it is my duty to check websites are appropriate for children before using them for educational purposes
- I know that password and settings are not to be altered without prior authorisation from Mrs Cichowska or SLT
- I must obtain permission from Mrs Cichowska to use tablets off school premises
- The tablet I use remains the property of Stoughton Infant School and is only to be used by the member of staff it is issued to
- If taken off the school premises, it is your responsibility to keep the tablet safe. The insurance does not cover accidental damage or theft from an unattended car. In these cases, it will be your responsibility to replace it
- All E-safety policies apply to tablets/iPads/Chromebooks

I agree to follow this code of conduct and to support the safe use of IT throughout the school. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation's most recent Acceptable Use Agreement (AUA).

Member of Staff full name: ……

Signature: …… Date: ……..