Stephenson Memorial Primary School - Online Safety Policy

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2022/3 (KCSIE), ‘Teaching Online Safety in Schools’ 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school’s safeguarding and child protection procedures.

Designated Safeguarding Lead (DSL)	Kerry Lilico
Online-safety lead & Deputy Safeguarding Lead	Lynsey Carr
Online-safety / safeguarding link governor	Brett Devenish
Computing Lead	

PSHE/RSHE lead	Lindsey Adams
Network manager / other technical support	Daniel Duthie
Date this policy was reviewed and by whom	July 2023 - Lynsey Carr
Date of next review and by whom	July 2024 - Lynsey Carr

The policy will be communicated in the following ways:

Posted on the school website
Available on the internal staff network/drive
Part of school induction pack for all new staff (including temporary, supply and non- classroom-based staff)
Integral to safeguarding updates and training for all staff
Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers

This policy aims to:

Set out expectations for all community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform

Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online

Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

○ *for the protection and benefit of the children and young people in their care, and*
○ *for their own protection, minimising misplaced or malicious allegations and to better*

understand their own standards and practice
○ *for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession*

Key responsibilities:
Headteacher & Online Safety Lead

Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding

Ensure that policies and procedures are followed by all staff

Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships

Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information

Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles

Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised

Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures

Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

Ensure the school website meets statutory requirements

Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns

Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance

Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents

Communicate regularly with SLT and the designated safeguarding and online safety committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/ helping.

Key responsibilities: Computing & RSE Lead

Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."

This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.

Technical – infrastructure / equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

There will be regular reviews and audits of the safety and security of school technical systems. Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school technical systems and devices.

All users will be provided with a username and secure password. Daniel Duthie / Lynsey Carr will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every quarter.

The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

Daniel Duthie is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

There is a clear process in place to deal with requests for filtering changes. The school has provided enhanced / differentiated user-level filtering

School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.

The school infrastructure and individual workstations are protected by up to date virus software.

An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

An agreed policy is in place) regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.

Use of Mobile Phones in School:

Pupils/students Only students in **Year 5/6** are allowed to bring mobile phones in for emergency use only. During lessons, phones must remain turned off at all times and kept safely by an adult.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours.

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos - unless with permission from Headteacher/Online Safety Lead.

Digital Images:

The use of digital images must depend upon the appropriate permission given by parents. All photographs/videos should be taken on a school device and once uploaded/emailed, deleted from the device.

Training - School Staff

All school staff receive an online safety update at least once each half term, access to Safer Schools, regular emails and bulletins. It is the responsibility of the Online Safety Lead to ensure that School Staff have the most up to date training and information.

Training - Governors

Regular updates during meetings, reports of online safety data and relevant training.

Training - Parents

Many parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

• Curriculum activities • Letters, newsletters, website • Parents / Carers evenings / sessions • High profile events / campaigns eg Safer Internet Day • Safer Schools App • Webinars

Reporting Online Safety Concerns:

Staff - Report to DSL or Online Safety Lead - via CPoms. (If a Cause for Concern then a conversation must be held too)

Children - Report to an adult who will then follow the above process.

Parents - Report to a member of staff who will then seek advice from the DSL or Online Safety Lead.

Additional Resources

https://www.ceop.police.uk/Safety-Centre/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://www.childnet.com/

https://nationalonlinesafety.com/