STANBURN PRIMARY SCHOOL

Online Safety Policy

Review Date:	**09/01/2025**
Reviewed By: (Committee Name)	**Headteacher**
Next Review Date:	**09/01/2027**
Name and Signature:	**Mark Lynch and Rabia Malik**

Stanburn Primary School
Online Safety Policy
(Managing the Internet Safely)

This policy is not a standalone document and should be read in conjunction with the school's **Acceptable Use Policy, Social Media Policy, GDPR Policy and Computing Policy.**

This policy applies to all members of the Stanburn Primary School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Roles and Responsibilities:

Headteacher: Elaine D'Souza	• Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding • Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
Designated Safeguarding Lead R Malik Online Safety Lead: M Lynch CPO	• Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify intervene in and escalate any incident where appropriate." • See DSL roles and responsibilities • Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents • Stay up to date with the latest trends in online safety • Review and update this policy
Governing Body Safeguarding and Online Safety Link Governor: Mrs K Patel	• Approve this policy and strategy and subsequently review its effectiveness • Support the school in encouraging parents and the wider community to become engaged in online safety activities
PSHE/RHE Lead: Mrs G Raine/Mrs K Hartland	• Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum
Computing Leads: Mr D Rafferty Miss R Rahanu	• Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum

	• Work closely with the Designated Safeguarding Lead /Online Safety Lead and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
Network manager: Wibird Stuart Lamond	• Keep up to date with the school's online safety policy and technical information • Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the Designated Safeguarding Lead and senior leadership team • Manage school network, and associated filtering and security systems
Data Protection Officer: DPO Centre	• see GDPR policy
All staff	• Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up • Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up • Sign and follow the staff acceptable use policy and code of conduct/handbook • Notify the Designated Safeguarding Lead /Online Safety Lead if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon • Identify opportunities to thread online safety through all school activities • Model safe, responsible and professional behaviours in your own use of technology and social media; to not bring school into disrepute
Subject Leaders	• Look for opportunities to embed online safety in your subject or aspect
Pupils	• Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually • Know what action to take if they or someone they know feels worried or vulnerable when using online technology
Parents	• Consult with the school if they have any concerns about their children's and others' use of technology • Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

AIMS:

This policy aims to:

- Set out expectations for all Stanburn Primary School 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 and respectful 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;
- 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).

Prevention Including Technical and Infrastructure approaches

This school:

- Has an internet connectivity with filtering and firewall services provided by the LGfL;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. Changes to the filtering policies are only available to staff with the approved 'web filtering management' status; Weekly Web usage searches are conducted and the Headteacher informed.
- Ensures the network protected by antivirus software. Sophos anti-virus software is provided by the LGfL and is installed on all computers;
- Uses individual log-ins for all users - the LGfL USO system; with the exception of children in Reception and Year 1 who use a generic logins to introduce them to the concept of usernames and passwords;
- Where sensitive data is to be transferred out of the school building precautions will be taken to ensure the security of this data. This would include the use of secure services such as S2S, USO FX and LGfL StaffMail;
- Staff should only use school devices for professional purposes;
- Is able to block Internet access on an individual basis through the school's Technical Support Provider;
- Provides a secure and monitored environment for sending and receiving emails, through the use of the school's VLE, staff do not engage in private email conversations with pupils;
- Provides staff with an email account for their professional use (London StaffMail) and makes clear personal email should be through a separate account;
- Provides staff with a Microsoft 365 account for use with Microsoft services including email and Teams;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Computing Leader and Technical Support Provider are up-to-date with LGfL services and policies;
- Pupils are aware that:
    - only pupils in Years 5 & 6 are permitted to bring in mobile phones, and only if they walk home alone;
    - they must be handed in to the teacher at the beginning of the day;
    - pupil use of mobile phones is not permitted on site.

Policy and procedures

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and pupils understand that they must report any concerns;
- Ensures pupils only publish within the appropriately secure school's MLE;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's MLE as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or kids search ;
- Is vigilant when conducting 'raw' image search with pupils;
- Informs users that their use of the school's Computing systems and the Internet is monitored by Securus software;
- Informs pupils and staff that that they must report any failure of the filtering systems directly to their teacher or the Online Safety Lead/DSL respectively. The school's Technical Support Provider logs or escalates as appropriate to LGfL as necessary;
- Requires pupils to agree to a pop-up acceptable use / e-safety message after each login, which is fully explained and used as part of the teaching programme;
- Requires all staff to sign a Staff Use of Computing Systems Agreement and keeps a copy on file;
- Ensure all adults onsite receive appropriate safeguarding training, which includes online safety;
- Ensures parents provide consent for pupils to use the Internet at the time of their child's entry to the school;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officers have appropriate training;
- Provides online safety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA;
- online safety concerns are no different to any other safeguarding concern;
- In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Education and training

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or Online safety lead/DSL;
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive online safety education programme throughout all year groups. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;

- to skim and scan information;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling, and include up-to-date information about other potential issues (e.g. online games, sexting, upskirting, online bullying, social media incidents);
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes online safety training available to staff;
- Runs a rolling programme of advice, guidance and training for parents, including:
  - suggestions on updating home ICT systems and ensuring filtering is in place;
  - demonstrations, practical sessions held at school;
  - access to 'think u know' materials;
  - suggestions for safe Internet use at home.

Cloud Platforms

This school:

- Continually assesses the suitability of the cloud-based platforms it uses;
- Engages the schools DPO to ensure that those cloud-based platforms are compliant with GDPR and that data stored on those platforms is included in the GDPR Information Asset Register;
- Assesses the security of its cloud-based services to minimise the risk of a data breach. This includes determining where it is appropriate to implement 2 factor authentication;
- Conducts regular staff training to re-enforce good practice around the use of cloud-based services and data security in general;
- Ensures that pupils and staff who use cloud based services have a clear understanding of good practice surrounding the sharing of data;
- Takes the opportunity of implementing new cloud based services to remind staff and pupils of the importance of keeping their password secret and changing it if they believe someone else might know what it is. This also includes advice on how to choose a strong password and how to avoid internet scams;
- Regularly reviews the systems that are being used to ensure they remain relevant, secure and are used appropriately.