Stoughton Infant and Nursery School

Northmead Junior School

Northmead
Junior School

Online Safety Policy

Date Agreed: 01/2026

Reviewed By: LGB

Next Review Due: 01/2027

Review Cycle: Annual

Learning Partners
academy trust

At Stoughton and Northmead Schools, safeguarding is our highest priority. Online safety forms part of our safeguarding responsibilities.

Our schools aim to:

- Have robust systems in place to ensure the online safety of all pupils, staff, volunteers and governors.
- Deliver a high-quality online safety curriculum.
- Establish clear processes to identify, intervene and escalate an incident, where appropriate.

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
Contact – being subjected to harmful online interaction with other users, such as child-on-child abuse, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

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 schools.

Roles and Responsibilities

Local Governing Board

The LGB will:

- Ensure this policy is being implemented.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the schools' community. The day-to-day responsibility for online safety will be delegated to the Online Safety Leader.

- 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 Leader 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 provides support to those colleagues who take on important monitoring roles.

The Designated Safeguarding Leads (DSL):
Details of the DSLs are in the Child Protection and Safeguarding policy.

The DSLs:

- Are trained in Online Safety issues and are 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
- Ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Work with the Online Safety Leader to deliver training for staff.
- Liaises with other agencies if necessary.
- Ensure any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and recorded on CPOMS.
- Receives reports of online safety incidents.

Online Safety Leader

● 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.
● Provides training and advice for staff and parents.
● Attends regular meetings regarding Internet Safety updates and issues.

ICT Manager

The ICT manager is 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.

● 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 schools' policies.

Staff and volunteers

All staff, including contractors, agency staff and volunteers will:

- Only use approved email accounts and should use Egress when emailing sensitive data outside of the school domain.
- Obtain permission from parents before publishing photos of pupils on newsletters, social media etc.
- Adhere to Learning Partners Academy Trust guidance in regard to collecting and storing data.
- Demonstrate that they have read and understood the Staff Acceptable Use Policy and Agreement (AUP).
- Report any suspected misuse or problem to the Head teacher or Online Safety Coordinator for investigation.
- Ensure that online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure that 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.

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. 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

Use of the internet is an essential element of 21st century life for education, business and social interaction. Stoughton and Northmead schools have a duty to provide students with quality computing experiences as a part of their learning and to cover online safety as part of the curriculum.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable online behaviour.
- Identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet is also covered. Online safety forms a part of the computing curriculum in every year group.

The schools also use assemblies to raise pupil's awareness of the dangers that can be encountered online and information is provided to parents through workshops and newsletters.

Remote and Hybrid Learning Safety

- Where a child needs to work from home, online learning may be provided.
- Pupils, staff, and parents will receive clear guidance on expected online behaviour, including appropriate use of cameras, microphones, and chat functions.
- Parents will be supported with guidance on monitoring online activity and setting up effective parental controls.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly by the Safeguarding Lead and the Computing Lead.
- Virus protection will be updated regularly.
- Headteacher and Deputy Headteachers receive 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)
- Regular checks are made using Securely Filtering System to monitor research made by all staff and pupils.
- In liaison with the Learning Partners guidelines, security strategies will be reviewed and updated as necessary.

Mobile Technologies

- The school Acceptable Use Agreements for staff and parents/carers considers the use of mobile technologies.
- We ask that mobile phones not be used during lessons or the school day, unless required for Multi-Factor Authentication.
- Only children in Years 5 and 6, with permission to walk home are allowed to bring in a mobile phone. Mobile phones will be locked away during the day.

E-mail

- Staff to parent email communications must only take place via a school email address.
- Staff to external agencies/ professional's emails must not contain any personal information e.g. a child's full name. Where necessary emails should be password protected using Egress Switch.

Social networking

- Access to social networking sites for children will not be permitted in school.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Staff and pupils should ensure that their online activity, both in school and out considers the feelings of others and is appropriate for their situation as a member of the school community.
- Where parents have taken photos during school events e.g. class assembly and Christmas play etc, parents will be asked to ensure that they do not share these photos on social media.

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.

Protecting personal data

There is a separate Data Protection Policy.

Authorising internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school electronic device or accessing emails.
- 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.

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.

Handling E-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff in line with the behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school's child protection procedures
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the Internet, and this will be in line with the school's behaviour policy
- All staff members can log behaviour and safeguarding issues related to online safety via

  CPOMS.

Communication of the policy

To pupils

- Appropriate elements of the E-safety Policy will be shared with pupils.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils.

Staff

- All staff will be shown where to access the school e-safety policy.
- 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.
- Staff will receive online safety training.

Parents

- Parents and carers will be provided with online safety updates in newsletters and can access this policy on the website.