



The Stalyhill Schools' Federation – Infant School

E-Safety Policy

Date of last review:	Spring 2026
Committee:	Full Governing Body
Date of next review:	Spring 2028
Policy Reference Number:	604

At Stalyhill Infants we will continuously strive to ensure that everyone is treated with respect and dignity. Each person will be given fair and equal opportunities to develop their full potential regardless of their gender, transgender, ethnicity, culture and religious background, sexuality, disability, or special educational needs and ability. The school will actively promote equality and foster positive attitudes and commitment to an education for equality.

Writing and reviewing the E-safety policy

The E-safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Positive behavior and anti-bullying and for Child Protection and Safeguarding.

The school will identify a member of staff who has an overview of E-safety, this would usually be the Senior Designated Professional (SDP).

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

Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of **E-Safety Governor**. The current E-Safety Governor is Sue Clark.

The Senior Leadership Team:

- ensures that all staff are aware of the procedures that need to be followed in the event of an e- safety incident taking place.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- provides advice for staff and others and organises training as needed
- liaises with external agencies, particularly in respect of child protection issues arising from e- safety work
- is a member of the E-Safety Committee.

The E-Safety Co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- keeps up-to date with developments in relation to e-safety and disseminates these widely
- helps ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- helps provide training and advice for staff and others
- liaises with teaching and other staff in developing and evaluating e-safety educational programmes
- liaises with the Local Authority / other relevant bodies
- liaises with school technical staff.

Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack, including regular updating of virus protection
- that the filtering system is applied effectively and consistently
- that user names/ access to school systems are updated e.g. when a member of staff leaves
- that checks are carried out as required on staff laptops
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- they read, understand and sign annually the Staff Acceptable Use Agreement (AUA) (Appendix Two)
- they report any suspected misuse or problem to the Headteacher/ E-Safety Coordinator / Officer
- all digital communications with students / pupils / parents / carers are on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- personal data is handled securely (see e-mail and Data Protection sections below)
- pupils understand and follow the e-safety and acceptable use policies
- pupils have an understanding of digital literacy and copyright issues appropriate to their age.

Teaching and Learning

Why Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Internet use enhances learning

Pupils are required to return a signed copy of the iPad Rules Agreement for Pupils every year, which must be countersigned by their parent or carer (in the case of Foundation Stage, parental signature only required).

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, using a 'child-friendly' search engine.

A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited using a variety of approaches appropriate to the age and maturity of the children.

Pupils are helped to understand the need for the pupil iPad Rules and encouraged to adopt safe and responsible use both within and outside school.

Pupils will be taught how to evaluate Internet content/ Digital Literacy

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils are taught to question information before accepting it as true.

Pupils are encouraged to tell a member of staff immediately if they find any material that makes them feel uncomfortable.

Educating parents and other carers

Many parents and carers may have only a limited understanding of e-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, school web site

Reference to other relevant web sites / publications

Education and training for staff

A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.

All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.

This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days at least annually.

The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

All staff will sign our ICT Acceptable Use Agreement on appointment and this will be included in induction packs for volunteers and students.

Governor education and training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection.

This may be offered in a number of ways e.g: Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.

Participation in school training / information sessions for staff or parents.

Governor monitoring visits will take place during the year and be reported to the Board of Governors.

Managing Internet Access

Information system security

School ICT systems security will be reviewed regularly.

Virus protection will be updated regularly.

Local Authority security strategies will be followed if appropriate.

E-mail

Staff and pupils may only use approved e-mail accounts on the school system.

Pupils must have adult supervision if using email. Pupils must immediately tell a teacher if they receive offensive or bullying email or any communication which makes them feel uncomfortable. They should not respond to such emails.

Staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Staff must immediately tell the Head teacher if they receive offensive or bullying email or any communication, which makes them feel uncomfortable. They should not respond to such emails.

E-mail sent to an external organisation should be professional in tone and content, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Senior Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate.

All parents are required to sign to say that images of their children can be used. Any photo titles or captions will not include children's surnames.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that students / pupils are appropriately dressed.

Social networking and personal publishing/Cyber-bullying

Staff, volunteers and students follow the guidelines in the Using Social Media Responsibly Policy. All staff are expected to have read this policy and to abide by the guidance. Failure to abide by the guidance could result in disciplinary action.

The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details 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 is inappropriate for primary aged pupils.

Any incidents of cyber-bullying will be reported directly to the Designated Safeguarding Lead. Any outside agencies such as police will then be notified, child protection procedures will be followed. Any pupil found to be involved with any misuse of the internet at school or home (including cyberbullying) will have their access to the internet taken away and this will be reviewed regularly. All incidents will be logged and regularly monitored, parents will also be informed.

Other members of the school community affected by cyberbullying should also be supported by the school.

Managing filtering

The school filtering system is provided by Foresight. An additional filtering and monitoring system provided by Senso is used for constant filtering and monitoring of IT devices with immediate emailed alerts to SLT. The system is tested termly and reported to Governors.

The school will work with the ICT support technician and LA to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the Computing Subject Leader and E-Safety Co-ordinator.

The Computing Subject Leader/ E-Safety Co-ordinator will ensure that regular checks are made so that the filtering methods selected are appropriate, effective and reasonable.

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 mobile phones are not to be used in the classroom during contact time. Staff cameras and other mobile devices are not to be used during contact time except for trips in order to contact school.

Staff are permitted to take their own mobiles with them on trips in case of personal emergency but they are not to be used routinely.

Parent helpers and others (students, volunteers will be reminded about school policy on phones and cameras when on trips.

Additional management is included on the Federation's Mobile Phone Policy

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. See Appendix Seven (Privacy Notice given to new parents)

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Complete Freedom of Information requests within the required timeframe
- When personal data is stored on any portable computer system, memory stick or any other removable media:
 - the data must be encrypted and password protected
 - the device must be password protected.

Use of school ICT equipment away from school premises

The provisions of this policy apply equally to all school ICT equipment when used away from school premises.

Assessing risks

Access to the internet will be by adult demonstration with directly supervised access to specific online resources.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Tameside LA can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Complaints

Responsibility for handling incidents of internet misuse will be taken by the E-Safety Officer/ Co-ordinator.

Any complaint about staff misuse of digital technology must be referred to the Head teacher.

Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.

Pupils and parents will be informed of the complaints procedure.

There may be occasions when discussions will be held with the police support services to establish procedures for handling potentially illegal issues.

Where possible the school will liaise with local organisations to establish a common approach to e-safety.

Communicating the E-Safety Policy

Introducing the e-safety policy to pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy

All staff will be given the School E-Safety Policy and Social Networking Policy and their importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

If a colleague at the school believes they will have any difficulty complying with any of the requirements in this policy for whatever reason (for example, where they are related to a pupil), they should discuss the matter with the Headteacher/ the school designated safeguarding teacher/officer. Failure to do so will be regarded as a serious matter.

Parental support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school web site.

Parents will be asked to read through the relevant iPad Rules Agreement for Pupils with their child and co-sign it on an annual basis.

Live Zoom calls

During a whole school closure due to the Coronavirus pandemic, school will host weekly Zoom calls between the children in school and the children learning from home. All procedures set out in the Risk Assessment will be followed. (See Appendix 1)

Ratified by Governors *Signed*.....

Date Reviewed annually



Reception iPad Rules



Our rules help us to stay happy and safe using the iPads

- When using the iPad with a teacher I will only use the app I am asked to use.
- I can use the iPads when I am planning to play and learn on different apps.
- I can use the iPads in the different areas to take photos.
- I will always be careful with the iPads and other ICT equipment.
- I will take turns with other children.
- If I break these rules I will not be able to use the iPads when I am planning.
- If I see anything that upsets me, or something I don't understand I will press the screen off button and tell an adult.



Completion of this form is mandatory to ensure school comply with their safeguarding duties.

Signed (parent): _____

Child's Name: _____



Year One iPad Rules



Our rules help us to stay happy and safe using the iPads

- When using the iPad with a teacher I will only use the app I am asked to use.
- I can use the iPads with permission when it is my turn to plan.
- I will not click or tap anything that I do not understand.
- I will always be careful with the iPads and other ICT equipment.
- I will take turns with other children.
- If I break these rules I will not be able to use the iPads when I am planning.
- If I see anything that upsets me, or something I don't understand I will press the screen off button and tell an adult.



Completion of this form is mandatory to ensure school comply with their safeguarding duties.

Signed (parent): _____

Signed (child): _____



Year Two iPad Rules



Our rules help us to stay happy and safe using the iPads

- I will always be careful with the iPads and other ICT equipment.
- When using the iPad with a teacher I will only use the app I am asked to use.
- If I would like to use the iPad to help with my work I will ask permission first.
- I will not click or tap anything that I do not understand.
- I will ask for help from an adult if I am not sure what to do or think I may have done something wrong.
- If I see anything that upsets me, or something I don't understand I will press the screen off button and tell an adult.
- I will follow the SMART rules:
Safe, Meeting, Accepting, Reliable, Tell.



Completion of this form is mandatory to ensure school comply with their safeguarding duties.

Signed (parent): _____

Signed (child): _____

Appendix 1 – Zoom risk assessment

Hazard/Risk	Who is at risk?	How can the hazards cause harm?	Control Measures	Who is responsible?	Risk rating
Inappropriate material/words being visible/heard on screen	Children Parents Staff	Inappropriate images (e.g. art) or words may be visible in rooms around the house. Adults at home and in school must be alert to vocabulary being used.	Zooms must take place in an appropriate room with an appropriate background i.e. not the child's bedroom. Parents to ensure correct vocabulary is used, for example, no offensive language. Staff to ensure that sensitive information is not visible or discussed during a live Zoom.	Parents Staff	Low
Unknown people logging into the Zoom session	Children Parents Staff	Somebody unknown to the school is present in the Zoom call.	The ID and passwords are only for the use of Stalyhill Infant School parents and children. Parents accessing from home must enter their child's name. Staff will only allow entry to the meeting from the names of children in the class. Meeting ID's and passwords will be sent directly to parents and not communicated in any other way i.e. website. Passwords will be randomly generated by Zoom and not easy to guess.	Parents Staff	Low
Individuals being left in a vulnerable position	Children Parents Staff	Individuals being left on screen on their own, open to allegations.	School to implement a Zoom waiting room. Children must always be with an adult when on a Zoom from home to ensure technology is being used appropriately. Two members of staff to be online until the meeting ends.	Parents Staff	Low
Appropriate clothing to be worn	Children Parents Staff	Inappropriate clothing being worn which could cause distress or upset to others.	Staff to follow school code of conduct. Parents and children to be fully and appropriately dressed i.e. no pyjamas.	Parents Staff	Low
Staff conducting live meetings from home	Staff	Personal data visible Paperwork taken off site Personal laptops used Electronic data not secure	Personal laptops and equipment not to be used – only school equipment Consider space you are working in and ensure no personal data is visible All electronic data is kept safe and secure by encryption and passwords No personal data to be taken off site, contact details to be accessed via sims/shared server	Staff	Low
Sharing of personal details	Children Parents Staff	Personal data, including photographs, shared/visible via Zoom	Teacher's to set up meeting with their school email address No personal information to be shared on Zoom Parents reminded not to share any personal data when on live calls.	Parents Staff	Low
Inappropriate behaviour	Children Staff	Verbal abuse Grooming Inappropriate discussion	Children to be in a communal area with an adult present. Two members of staff present in all live feeds. Staff to act as a facilitator of the discussion. Staff to use zoom tools to limit the chat function. Staff to use waiting room to ensure the meeting is live only when the host is present.	Staff Parents	Low
Poor environment	Children Staff	Fatigue Stress Headaches Unable to see the screen properly	No obstructions Adequate lighting Adequate position of camera Zoom meetings limited to set time.	Staff Parents	Low
Recording/photographing the/parts of session	Children Staff Parents	Photographs, screenshots and recordings of people in the meeting being taken without permission.	The meeting will not be recorded unless participants are notified and consent gained. Photographs/screen shots must not be taken by any participant.	Staff Parents Children	Low