Shelton Infant School

Online Safety Policy

ICT Subject Leader: Dan Kershaw
Online Safety Leaders: Dan Kershaw, Anthony Leigh

Introduction
Shelton Infant School recognises that Online Safety is an integral element of Safeguarding and is, therefore, of paramount importance. The school also recognises that the digital world is constantly changing and evolving. The school is proud to have gained the 360 Degree Online Safety Mark in recognition of its provision for online safety and continues to use the 360 Degree Safe Review Tool to regularly monitor and self-evaluate our provision.

1. Why the Internet and digital communications are important

The purpose of Internet and digital communication use in school are to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet, digital media and digital communication use are part of the statutory curriculum and a necessary tool for staff and pupils.

Internet access is an entitlement for all pupils.

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

2. Teaching & Learning

Benefits of the internet and digital communication in education

- access to world-wide educational resources
- educational and cultural exchanges between pupils world-wide
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the Local Authority, Department for Education etc.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives and rules for Internet use – the school's "Online Safety Goals".

Staff will guide pupils in online activities that support the planned learning outcomes appropriate to the pupils' age and maturity.

Internet access will be planned to enrich and extend learning activities.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval as appropriate to the age of the pupils.

Pupils will be taught how to evaluate Internet content

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

Pupils will be taught how to report materials that they feel are distasteful, uncomfortable, unpleasant or threatening to an adult.

Some pupils may use the Internet widely outside school and therefore all pupils will be taught how to evaluate Internet information and to take care of their own safety and security.

3. Managing Internet Access

Managing school website content

The point of contact on the School Website is the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

The Computing Subject Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

Pupil's names will not be used on the school website. Parents may however post children's first names on the school Class Dojo feed and staff may subsequently post the children's first names when replying to Class Dojo feed posts.

Publishing pupil's images and work on the school website

Staff will ensure that only digital cameras or iPads provided by the school will be used to photograph pupils.

Staff will ensure that all photographs/videos of pupils are deleted from the school digital cameras / iPads as soon as practically possible once transferred.

Staff will ensure that no photograph or image of pupils will be transferred to personal or home computer systems (this also includes personal USB devices).

Written permission from parents or carers will be obtained before photographs and videos of pupils are published on the school website. This will be obtained when a pupil starts school. Pupil's names will not be used on the school website. Parents may however post children's first names on the school Class Dojo feed and staff may subsequently post the children's first names when replying to Class Dojo feed posts.

Work can only be published with the permission of the parents.

File names for pupils' photographs or work will not refer to the pupil by name.

Parents are clearly informed of the school policy on image taking and publishing, both on school and independent websites.

Specific written permission from parents or carers will be obtained before photographs of pupils are published on any other websites. Wherever possible, parents or carers will be provided with details of the website, together with a copy of the photograph and details of whether the child's name will be published.

Managing E-mail

Pupils will only use approved e-mail accounts on the school system in whole class or group activities which are adult led. Pupils will not use any e-mails accounts independently.

All e-mails sent to pupils will be opened by the member of school staff responsible for that account and the content assessed for its suitability for viewing by pupils before sharing the e-mail with pupils.

In e-mail communication, pupils' personal details or those of others will not be revealed.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school should consider how e-mail from pupils to external bodies is presented and controlled.

The forwarding of chain letters is not permitted.

All staff will be provided with a copy of 'Guidelines for Safe Use of School E-Mail Addresses' and make use of their e-mail accounts by following the guidelines. (Please see Appendix I.)

Social media/networking

For the purposes of this policy, social media is any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public form. This includes, but is not limited to, online social forums such as *Facebook, Twitter, Linkedin,* etc. Social media also covers blogs and video and image sharing websites such as *YouTube, Instagram, TikTok, SnapChat* etc.

Staff and pupils will not use the school's internet service to access social networking sites.

Pupils will be given opportunities to discuss social networking and safety issues surrounding it during online safety lessons.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils are advised not to place personal photos on any social network space.

Pupils are advised on internet safety and security through online safety lessons. Lessons will cover Internet related situations that the children may encounter in school and outside of school and may use materials published on the Internet by reputable providers including Purple Mash, UK Safer Internet, CEOP and 'Think U Know'.

Pupils will be advised on the use of avatars and nicknames when accessing the Internet.

Pupils are advised not to publish specific and detailed private thoughts, and personal photographs. Pupils are advised not to make contact with other users of the internet (eg in chatrooms) without adult supervision.

Staff must not run social network spaces for pupils use on a personal basis.

Staff must not accept or approach pupils, ex pupils or parents as 'friends/contacts' on social networking sites.

Staff must not share any personal information with any pupil, including personal contact details, personal website addresses or social networking site details.

Staff must not engage in any online discussion about any child attending (or previously attending) the school. Staff must not disclose any information that is confidential to the school or post anything that could potentially bring the school into disrepute.

Staff are strongly advised to take steps to ensure their online personal data is not accessible to anybody whom they do not wish to access it, eg,

they are advised to set security and privacy settings to their maximum level.

While the school does not discourage staff from using social networking sites, staff should be aware that the Board of Governors will take seriously any circumstances where such sites are used inappropriately and disciplinary action may be taken.

The 2025 guidance adds *disinformation* (the deliberate creation and spread of false or misleading content, such as fake news), *misinformation* (the unintentional spread of this false or misleading content) and *conspiracy theories* to the list of content risks under online safety.

Managing filtering

Control of filtering is via Schools Broadband, with the school able to adjust if necessary, via their Technician.

If staff or pupils come across unsuitable on-line materials, the site address must be immediately reported to the Online Safety Lead and / or Designated Safeguarding Leads (DSLs).

KCSIE 2025 includes a link to the DfE guidance Generative AI: product safety expectations. This guidance on generative artificial intelligence (AI) explains how filtering and monitoring requirements apply to the use of generative AI in education and supports schools to use generative AI safely.

In line with the requirements stated in Keeping Children Safe In Education (2024) the governing body and senior leadership team will regularly review the effectiveness of school filters and monitoring systems. At least annually a written audit of the school's filtering and monitoring systems will be completed by the school's senior leadership team in conjunction with the school's IT technician. This audit will be shared with the Governing Body.

They will ensure that the leadership team:
- are aware of and understand the systems in place
- manage them effectively
- know how to escalate concerns when identified.

The ICT Technician will make regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies.

Regular communications with parents and carers reinforce the importance of children being safe online.

The school will share information with parents/carers about:
- what systems are in place to filter and monitor online use
- what children are asked to do online, including the sites they will be asked to access

- who from the school (if anyone) their child is going to be interacting with online.

Managing webcam use

Webcam use with pupils will be appropriately supervised by a member of the teaching staff at all times.

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 may have mobile phones on their persons during the school day, however, they will be switched off at all times whilst they are with the children. Members of staff will not use mobile phones whilst they are with the pupils unless it forms a part of the lesson and with prior arrangement with the Headteacher or member of the Senior Leadership Team. In the case of family emergencies etc. where a member of staff is waiting for a call, staff will speak with the Headteacher or in his absence a member of the Senior Leadership Team, to gain permission that they may leave their phone on whilst with the children. Members of staff are not permitted, in any circumstances, to use their phones for taking, recording or sharing images.

Other Devices

The senior leadership team should note that technologies such as mobile phones and smart watches with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Pupils will not be allowed to bring personal mobile phones or smart watches with the capability to go online and take photographs/videos onto school premises.

Games machines including the Sony Playstation, Microsoft Xbox, Nintendo Switch and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

The Computing Lead regularly updates parents and carers about updates and relevant information linked to games consoles and so on, via the school Class Dojo feed.

Authorising Internet access

All staff must read and sign the “Staff Code of Conduct for ICT” before using any school ICT resource. (Please see Appendix III). Anyone not directly employed by the school but wishing to use the school’s ICT resources on a regular basis will also read and sign the code, e.g. ICT technician, speech therapists.

All staff must also read and sign the Learning Derby Acceptable use policy before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

For pupils, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form. (Please see Appendix IV).

Pupils will be made aware of and be required to follow the School Internet Rules for children – the "Online Safety Goals".

The Prevent duty

All schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism**.** This duty is known as the 'Prevent' duty. Terrorism is defined as not just violent extremism, but also non-violent extremism that can create an atmosphere conducive to terrorism and popularise views which terrorists exploit.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Through regular safeguarding training, all staff are aware of the risks posed by the online activity of extremist and terrorist groups.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

The Online Safety Lead and DSLs will ensure that this policy is implemented and complied with at all times.

4. Communicating the Policy

Introducing the online safety policy to pupils

E-Safety rules (“Online Safety Goals”) will be posted in all rooms where computers are used and discussed with pupils regularly. (Please see Appendix V).

Pupils will be informed that Internet use is always monitored.

Online Safety is embedded within the school's Computing curriculum. The Online Safety knowledge and skills will be taught to the children via Purple Mash 2BeSafe – a comprehensive online safety scheme aligned with the Education for a Connected World framework.

Online Safety Policy & Parents

Parents’ attention will be drawn to the School Online Safety Policy in in newsletters and on the school website.

The Online Safety Lead will advise parents on how they can obtain further online safety information and support from external agencies should they require. This will be via regular notifications on the school website, through Class Dojo and the school twitter account.

Internet issues will be handled sensitively to inform parents without undue alarm. Any issues raised by parents will be recorded and addressed as quickly as possible (see Appendix VI).

The school will ask all new parents to sign the parental agreements for using the internet and publishing photographs/videos on the school website and twitter feed when they register their child with the school.

Staff and the Online Safety policy

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing Body will make sure all staff receive online safety training as part of child protection and safeguarding training, ensure staff understand their expectations, roles and responsibilities around filtering and monitoring, make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Chair of Governors will liaise with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards.

The governor who oversees online safety is Mrs Gill Hall (Chair of Governors).

All teachers and teaching assistants will be given a copy of the School Online Safety Policy.

Staff must be informed that network and Internet traffic can be monitored and traced (and in some instances to the individual user). Discretion and professional conduct are essential.

Staff that manage filtering systems or monitor ICT use will be supervised by the Headteacher and Online Safety Leader and work to clear procedures for reporting issues.

Internet searches made by children will always be supervised by a member of staff.

Training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

All staff will sign to confirm that they have read and agreed to abide by the Staff Code of Conduct for ICT.

5. Maintaining ICT system security

School ICT systems will be reviewed regularly with regard to security.

Virus protection will be installed and updated regularly.

All Internet connections are connected via the Schools Broadband network.

Security strategies will be discussed with the Local Authority.

The server operating system is secured and kept up to date.

Personal data sent over the Internet or carried on portable media will be encrypted or otherwise secured.

Personal portable storage devices may not be brought into school and used without specific permission and a virus check.

6. Handling online safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred immediately to the headteacher.

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

Pupils and parents will be informed of the complaints procedure (see schools complaints policy). The complaints policy will be published on the school website.

Discussions will be held with the Derby Safeguarding Children's Board to establish procedures for handling potentially illegal issues/criminal offences.

Statutory Framework

This policy has been devised in accordance with the following legislation and guidance:-

- Keeping Children Safe in Education (September 2025) DfE
- Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children (Decembetr 2023) DfE
- The Prevent Duty – Departmental advice for schools and childcare providers (April 2023) DfE
- The Derby and Derbyshire Safeguarding Children procedures

Policies

This policy links to other policies -
Safeguarding
Code of Safe Conduct for Staff & Volunteers
Personal, Social, Health and Citizenship Education
Health and Safety
Anti-bullying
Whistleblowing
Confidentiality

This policy was reviewed by all staff and governors in September 2025 and will be reviewed again by the staff & governors no later than September 2026. It will be reviewed earlier if incidents/circumstances deem this necessary. A copy of this policy forms part of the induction pack for all people who work with ICT in school including students.
All staff who access ICT within the school are also required to read and sign the school's Staff Code of Conduct for ICT (Appendix III).

Signature _____ Headteacher Date _____

Signature _____ Chair of Governors Date _____

Shelton Infant and Nursery School

APPENDIX I

Guidelines for Safe Use of School E-Mail Addresses

These guidelines should be read in conjunction with the school's Data Protection Policy and the school's Online Safety Policy.

1. Confidential information e.g. assessment records or any document with a child's name should only be sent via the school's secure email system.

2. Anything relating to child protection must not be sent via e-mail unless using the Local Authority's secure 'Egress' email system.

3. Personal e-mail accounts must not be accessed using computers connected to the school's internet connection.

4. E-mails sent to outside organisations and people outside of the school (e.g. within the council) should be sent from a school e-mail address.

5. School e-mail accounts need to be used for communication related to school only. Do not register on websites that do not relate to school activities using a school e-mail address.

-

Shelton Infant and Nursery School

APPENDIX II

Data Protection Guidelines

- Any electronic files containing personal and/or sensitive data need to be treated as confidential.

- Personal data is any information that can potentially identify a living individual, even if their name is not included but there is enough information to identify them.

- Sensitive data includes information on racial or ethnic origin, political opinions, religious or other beliefs, health, sexual life, criminal allegations, proceedings or convictions.

- Electronic files that have confidential information or personal and sensitive data can only be stored on PCs and laptops that have encrypted software installed.

- Electronic files that have confidential information or personal and sensitive data can be stored on encrypted memory sticks only.

- Confidential information should not be sent via e-mail.

- For any confidential information that has to be sent outside the school please use non-electronic methods or if necessary encrypted memory sticks.

- Any storage devices that contain personal or sensitive information that are no longer being used or are no longer appropriate for storing such

information (e.g. disks, old laptops etc) should be given to the Computing Lead for suitable formatting/recycling.

Shelton Infant and Nursery School

Staff Code of Conduct for ICT and Online Safety (Appendix III)

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's online safety policy for further information and clarification.

- I have received, read and understood a copy of the school's Online Safety policy and relevant appendices
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

· I appreciate that ICT includes a wide range of systems, including smartphones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
· I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
· I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
· I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
· I will not install any software or hardware without permission.
· I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
· I will respect copyright and intellectual property rights.
· I will report any incidents of concern regarding children's safety to the Online Safety Lead or the Designated Safeguarding Leads.
· I will ensure that electronic communications with pupils including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
· I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be

being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT and Online Safety

Sign ... Name ... Date ...

Online Safety and Internet Access Rules and Consent for Use of Pupils' Photographs (Appendix IV)

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum and the Early Years Foundation Stage Curriculum. Parents/carers are asked to sign to show that the Internet/Online Safety Rules have been understood and agreed. Pupils' photographs and videos are published using our school website and school Class Dojo feed. Parents/carers are asked to sign below to consent to their child's photographs/videos being published on the school website and the school's Class Dojo account.

Parents/Carers Consent

I have read and understood the school online safety/internet rules and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I give permission for my child's photographs (and videos featuring my child) to be published on the school's website and on the school's Class Dojo account. I understand that my child will not be named in these photographs or videos.

Name of child: ***Class:***

Signed: *(parent/carer)*	***Date:***
Please print name:	

Shelton Infant and Nursery School

Online Safety Goals

These rules help us stay safe online:

Keep your password safe and sound.

Keep your name and address and other

personal information to yourself.

If you see something you think is wrong or upsetting, tell a grown up (teacher, mum, dad…)

Name of reporter: _____

Date concern raised: _____

Details:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____