SCAWSBY SALTERSGATE INFANT SCHOOL

E-SAFETY POLICY

Policy Approved by Governors	**April 2024**
Review Date	**April 2025**

Aims

- To set out the key principles expected of all members of the school community at Saltersgate Infant School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Saltersgate Infant School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the ICT technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality e.g. tablets, Xbox, Playstation

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Saltersgate Infant School we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Policy (for all staff, classroom based visitors and children) are inclusive of both fixed and mobile internet; technologies provided by the school (such as Ipads, laptops, webcams, interactive whiteboards, digital video equipment);

and technologies owned by pupils and staff, but brought onto school premises (such as tablets, laptops, mobile phones).

Roles and Responsibilities

We believe that E-Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team

- The Headteacher is ultimately responsible for E-Safeguarding provision for all members of the school community, though the day-to-day responsibility for E-Safeguarding may be delegated to the E-Safety provider and/or E-safety Coordinator (Designated Safeguarding Lead).
- The Headteacher, Designated Safeguarding Lead and Senior Leadership Team are responsible for ensuring that all staff receive suitable training to enable them to carry out their E-Safeguarding roles and to train other colleagues when necessary.
- The Senior Leadership Team will receive monitoring reports where necessary from the E-Safety provider and/or E-safety Coordinator (Designated Safeguarding Lead).
- The Headteacher and Senior Leadership Team should ensure that they are aware of procedures to be followed in the event of a serious E-Safeguarding incident.

Responsibilities of the E-Safeguarding Coordinator (Designated Safeguarding Lead)

- To promote an awareness and commitment to E-Safety throughout the school
- To be the first point of contact in school on all E-Safeguarding matters
- To take day-to-day responsibility for E-Safety within school and to have a leading role in establishing and reviewing the school E-Safety/Acceptable Use policies and procedures
- To have regular contact with other E-Safeguarding Committees, e.g. the Local Authority, Local Safeguarding Children Board
- To communicate regularly with school technical staff
- To communicate regularly with the designated person for Child Protection on matters related to E-Safety
- To communicate regularly with the Senior Leadership Team
- To create and maintain E-Safety policies and procedures
- To develop an understanding of current E-Safety issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in E-Safety issues

- To ensure that an appropriate E-Safety education is embedded across the curriculum
- To ensure that E-Safety is promoted to parents and carers
- To liaise with the Local Authority, the Local Safeguarding Children Board and other relevant agencies as appropriate
- To monitor and report on E-Safety issues to the E-Safeguarding group and the Senior Leadership Team as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safeguarding incident
- To ensure that an E-Safeguarding incident log is kept up to date

Responsibilities of the Governing Body

- To ensure that the school E-Safety policy is current and pertinent
- To ensure that the school E-Safety policy is reviewed at prearranged time intervals
- To ensure that school Acceptable Use Policies are appropriate for the intended audience
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school
- To read, understand, contribute to and help promote the school's E-Safeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the Headteacher, E-safety Coordinator (Designated Safeguarding Lead) and SLT in promoting and ensuring the safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safeguarding activities
- To ensure appropriate funding and resources are available for the school to implement its e-Safeguarding strategy.

Responsibilities of teachers and support staff

- To read, understand and help promote the school's E-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the E-Safety Coordinator (Designated Safeguarding Lead)
- To develop and maintain an awareness of current E-Safeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media e.g. Facebook etc.

- To embed E-Safety messages in learning activities across all areas of the curriculum
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of E-Safety issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of technical staff (this may be via an outside provider)

- To read, understand, contribute to and help promote the school's E-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any E-Safety related issues that come to their attention to the E-Safety Coordinator (Designated Safeguarding Lead)
- To develop and maintain an awareness of current E-Safety issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in the personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the Local Authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

- To ensure that controls and procedures exist so that access to school-owned software assets is restricted

Responsibilities of pupils

- To read, understand and adhere to the school's Pupil Acceptable Use Policy
- To adhere to any policies and practices the school creates
- To know and understand school policies on the use of mobile phones
- To know and understand school policies regarding cyberbullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To be fully aware of research skills
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To discuss E-Safety issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the school in promoting E-Safety
- To promote the school's Pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- To discuss E-Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology

- To refrain from uploading or sharing images of children taken at school events on social networking sites or other sites via the internet
- To provide written consent for the use of images of their children for different purposes e.g. press releases, school website etc.

Responsibilities of the Designated Person for Child Protection (DSL)

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose

Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to E-Safeguarding and the safe use of technologies
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school

Managing digital content

Using images, video and sound

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done on entry to the school. Use of images may include:
    - On the school website
    - In the school prospectus and other printed promotional material, e.g. newspapers
    - On displays around school
    - Use on social media
- Parents and carers may withdraw permission, in writing, at any time

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the Headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved
- If pupils are involved, relevant parental permission will also be sought before resources are published online
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites. Parents are reminded of this at the start of any school event.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment. A dedicated area is available on the school network for this
- The school will store images of pupils that have left the school for 2 years following their departure for use in school activities and promotional resources
- Pupils and staff are not permitted to use personal portable media (memory sticks) for storage of any images, videos or sound clips of pupils
- The class teacher and year group leaders have the responsibility of deleting the images when they are no longer required, or when a pupil has left the school. This is advised at the start of each academic year

Learning and teaching

- We will provide a series of specific E-Safeguarding-related lessons in every year group / specific year groups as part of the ICT curriculum / PSHE curriculum / other lessons. This includes our PREVENT duty. http://intranet.doncaster.gov.uk/directorates/adults-health-wellbeing/preventing-people-being-drawn-into-extremism

- We will discuss, remind or raise relevant E-Safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way
- Staff will model safe and responsible behaviour in their own use of technology during lessons
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content
- Pupils will be taught about the impact of cyberbullying in an age appropriate way and know how to seek help if they are affected by any form of online bullying
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member

Staff training

- Our staff receive regular information and training on E-Safeguarding issues in the form of staff meetings and policy updates
- As part of the induction process, all new staff receive information and guidance on the E-Safeguarding policy and the school's Acceptable Use Policies
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safeguarding and know what to do in the event of misuse of technology by any member of the school community. They should inform the Headteacher and/or the E-Safeguarding Coordinator (Designated Safeguarding Lead).
- All staff will be encouraged to incorporate E-Safeguarding activities and awareness within their curriculum areas

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access
- Servers, workstations and other hardware and software will be kept updated as appropriate

- Virus protection is installed on all appropriate hardware, and will be kept active and up to date
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive
- All users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked
- All pupil internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system)
- Pupils will have a generic 'pupil' logon to all school ICT equipment
- All teaching staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school
- All information systems require end users to change their password at first log on
- Users should be prompted to change their passwords at any time that they feel their password may have been compromised
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access
- Staff will:
    - Not write down system passwords
    - Only disclose their personal password to authorised ICT support staff when necessary and never to anyone else.
    - Ensure that all personal passwords that have been disclosed are changed as soon as possible
    - Always use their own personal passwords to access computer based services, never share these with other users
    - Make sure personal passwords are entered for each logon. Do not include passwords in any automated logon procedures
    - Never save system-based usernames and passwords within an internet browser
- All access to school information assets will be controlled via username and password
- No user should be able to access another user's files unless delegated permission has been granted

- Access to personal data is securely controlled in line with the school's personal data policy
- Users should create different passwords for different accounts and applications
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Doncaster Council
- The school's internet provision will include filtering appropriate to the age and maturity of pupils
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision
- If users discover a website with inappropriate content, this should be reported to the Headteacher and/or the E-Safeguarding Coordinator (Designated Safeguarding Lead). All incidents should be documented
- If users discover a website with potentially illegal content, this should be reported immediately to the Headteacher and/or E-Safeguarding Coordinator (Designated Safeguarding Lead). The school will report such incidents to appropriate agencies including the filtering provider, the Local Authority, CEOP or the IWF
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked
- Pupils will be taught to assess content as their internet usage skills develop
- Pupils will use age-appropriate tools to research internet content
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum

PREVENT Duty

As a school, we have undertaken the PREVENT self-assessment and all staff are aware of spotting the signs, including when using ICT-based technologies.

- The school SMSC curriculum explores shared values and beliefs
- The school includes Educate Against Hate http://www.educateagainsthate.com/
- School leaders have completed a PREVENT self-assessment
- The Designated Safeguarding Lead has accessed Home Office approved WRAP training
- All staff access basic Prevent Awareness Training
- Staff are aware of the PREVENT agenda and understand the Doncaster Channel Process

The South Yorkshire Police PREVENT team are the first point of contact and also provide a response to any PREVENT related concerns - Prevent Inbox: Prevent_Inbox@southyorks.pnn.police.uk

- **Report Extremist Material:** https://www.gov.uk/report-terrorism
- **Preventing Terrorism:** www.ltai.info
- **Stay Safe Advice**: www.npcc.police.uk/staysafe
- **North East Counter Terrorism Unit:** www.northeastctu.police.uk
- **UK Anti-Terrorist Hotline Number:** 0800 789 321

Managing the school E-Safety messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The E-Safety Acceptable Use contract for parents and pupils will be included with the home school agreement when children start school
- E-Safety information is to be made available on the school website

E-Safety in the Curriculum

- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum
- Pupils are made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline
- Pupils are taught good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- The school will send out relevant E-Safety information for parents/carers through newsletters, website and the school prospectus

Data Security

The accessing of school data is something that the school takes very seriously.

Staff are aware of their responsibility when accessing school data. They will ensure that:

- secure/sensitive information is only stored on school equipment and is appropriately protected either by passwords or suitable encryption

- they understand their personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up. At Saltersgate Infant School, we will ensure:

- Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

E-mail (KS1)

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

Social networking and personal publishing - in line with Social Media Guidance Policy

- The school will block/filter access to social networking sites on school equipment

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However we accept that some pupils will still use them; they will be advised never to give out personal details of any kind which may identify them or their location
- Our pupils are asked to report any incidents of bullying to the school
- School staff are not to add children or parents as 'friends' if they use these sites. (Staff Code of Conduct, Social Media Policy for Education Establishment Staff)
- Staff will read and adhere to the Social Media Policy for Education Establishment Staff

Mobile technologies

- Many new and existing mobile technologies such as tablets, portable media players, gaming devices, mobile and smart phones are familiar to children outside school. Some now offer open access to the internet and therefore open up risks associated with unregulated internet access
- No use is allowed in school of the above technologies by pupils
- The school allows staff to bring in personal mobile phones and devices for their own use. Staff must ensure mobile phones are not used when children are present e.g. during contracted teaching time, unless there is an emergency and that phones are set to silent mode in order to minimise disruption during lessons. Under no circumstances will personal mobile phones be used to take images of children by staff. Personal mobile phones must not be used to communicate with parents about any children unless in an emergency situation. Personal contact details must not be passed to parents
- Mobile phone calls and text messaging will take place in staff's own time e.g. break times and where children are not present. For the comfort of all staff, please refrain from using mobile phones for personal telephone calls in the staff room

Assessing risks

- 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 DMBC 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

Handling E-Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff

- Any complaint about staff misuse must be referred to the Headteacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher and/or E-Safety Co-ordinator (Designated Safeguarding Lead)
- Depending on the seriousness of the offence; investigation by the Headteacher/LA may involve immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures

The E-Safety Policy and its implementation will be reviewed annually

This policy should be read alongside the Acceptable Use Policy, Safeguarding Policy and Social Media Policy.