



Online Safety Policy

Author: S.Evans
Issue Date: April 2020

To be reviewed: April 2021

Where possible we offer translation or explanation of written communication. Please contact the school office if you require forms/paperwork in any other format.

Writing and Reviewing the Online Safety Policy

The Online Safety policy is part of the School Development Plan and relates to the other policies including those for computing, bullying, safeguarding and child protection.

- The school will appoint the ICT/Computing Subject Leader as the Online Safety Co-Ordinator. They may on occasions, have to liaise with the Designated Safeguarding Lead, as the roles may overlap at times.
- Our Online Safety policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by the Governors and PTA.
- The Online Safety policy and its implementation will be reviewed annually.
- The Department of Education has published an updated version of its statutory safeguarding guidance, Keeping Children Safe in Education. The guidance includes information about safeguarding children online which provides the basis for this policy. The guidance explains in paragraph 87 that children should be safeguarded by from potentially harmful and inappropriate online material. Paragraph 90 states however that 'over blocking' does not lead to 'unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Teaching and Learning

Why Internet Use Is 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 statutory curriculum and a necessary tool for staff and pupils.

Internet Use Will Enhance Learning

The schools internet access will include filtering appropriate to the age of the pupils. This will be on all technology devices including Ipads and laptops.

- From the Early Years, pupils will be taught and given clear objectives for internet use through computing and PHSE teaching at least once a term each academic year.
- Pupils will sign a code of conduct at the start of the year to accept the computing terms set by Silsoe Lower School to use technology safely and respectfully throughout the year. Misuse of technology/internet will result in children having a "time-out" from using it in school. (Appendix 1). The code of conduct will also be sent home for parents to co-sign to involve them in online safety.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation through Online Safety lessons.

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 should be taught to be critically aware of the **content** materials they read and shown how to validate information before accepting its accuracy. They will also be taught about age appropriate content from video games, to YouTube videos.
- Pupils will be taught how to **conduct** themselves when looking at internet content and what to do in the event they discover content they deem to be inappropriate. They will be taught about the importance of keeping personal information private on all devices and apps.
- Pupils will be taught how to communicate safely using technology as a way of making **contact** with others through a variety of devices, programs and apps. They will also be taught about cyber-bullying and trolling and that when contacting others we must consider what we are saying.

Managing Internet Access

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly. Staff and Simply IT will ensure that their laptop virus protection is current and is updated regularly.
- Security strategies will be discussed with our service provider and our consultant technician.
- Staff are required to lock their screen/laptop when leaving it unattended to ensure data protection.
- Staff will use a unique login id and password, which will remain private and should be different from personal passwords. Passwords should be changed regularly at 3 monthly intervals.
- Pupils will use a unique login id with a common password.

E-mail

- Pupils may only use approved e-mail accounts on the purple mash/Google classroom portal. External access for pupil email will be blocked.
- Pupils must immediately tell a teacher or an adult if they receive offensive e-mail and this must be recorded in the Incident Log. Pupils can also report offensive emails to their teacher via the purple mash interface.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone with specific permission.
- The forwarding of chain letters is not permitted.

Published Content and the School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils work can only be published at the discretion of the class teacher.
- Photographs will only be taken using school equipment, stored in central secure location and deleted at regular intervals. Photographs of pupils should not be held on staff laptops but on the secure system.

Social Networking and Personal Publishing

- The school will filter access to social networking sites. Pupils will not have access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised through safety lessons never to give out personal details of any kind which may identify them or their location.
- Pupils will be taught how to conduct themselves appropriately when using social networking spaces via the purple mash school portal.
- Pupils and parents will be advised that the use of the social network spaces outside school is inappropriate for primary aged pupils.

Managing Filtering

- The school will work with the Local Authority, DfES and the internet service provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported immediately to the Online Safety Co-Ordinator and recorded on CPOMs.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The software Impero will be installed on all computer devices to monitor, lock and control the use of the internet/computer whilst children are using. This

supports staff to supervise and control all laptops in use. It also supports staff in capturing inappropriate use of technology

Managing Emerging Technologies

- Filtering is provided by our Simply -IT
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- When staff require mobile phone contact with other members of staff the school, or parent of the pupils of the visit when off site with pupils may use the school mobile phone.
- Pupils must not use/have smart technologies in school outside of teacher-led learning (including smart watches e.g. fitbits).

IPad Staff

- Staff must not use the iPad for personal use.
- Staff must not access any personal accounts on the iPad or change any settings.
- Staff must not bypass Silsoe VC Lower School's web filter through a web proxy.
- Staff must employ good judgement when using the camera, and do not use it to take inappropriate pictures or videos.
- Photographs of children must be saved onto the school system
- Staff must remember that the iPad desktop may be seen by pupils, so ensure that nothing inappropriate is visible.
- iPad must be kept safe and secure. Staff must report loss or damage to the device to the Head Teacher immediately.
- iPad must have protective covers at all times

IPad/ Pupils

- iPad should always be used with the protective case.
- iPad must only be used in the teaching environment.
- Pupils must not bypass Silsoe Lower School's web filter through a web proxy.
- Pupils must not download any software or access personal accounts.
- Pupils must understand their responsibilities and comply with the rules given by the teacher of using the internet whilst using the iPad
- Pupils must use all technology sensibly in an appropriate manner to avoid damage to the equipment and the school network system.
- Pupils must not change the iPad settings.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and recent GDPR compliances.
- Information will be classified accordingly to government classification levels and recorded in a classification log. Details will be reviewed as appropriate and maintained by the SIRO.
- Sensitive data should be held on a central secure location and not on staff laptops or USB storage devices.

Policy Decisions

Authorising Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up to date, for instance a member of staff may leave or a pupil's access is withdrawn.
- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on line materials.
- At Key Stage 2, access to the internet will be supervised with guidance towards specific, approved on line materials. Pupils will be taught about the safe use of search engines and selection of appropriate material.
- Parents will be asked to sign and return the Acceptable use of ICT by the pupils' consent form on joining the school.
- Children who are in KS1 and KS2 will sign a code of conduct at the start of every academic year to reinforce the expectations of Online Safety (appendix 1).

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, laptop or iPad.
- The school cannot accept liability for the material accessed, or any consequences of internet access, however any incidents will be reported to the safety coordinator and recorded in the incident log.
- The Online Safety Coordinator, in consultation with the network manager, will decide upon the appropriate action to be taken to prevent the situation arising again.
- The school will audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by the Online Safety Coordinator and recorded on CPOMS
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community Use of the Internet

- The School will liaise with local organisations to establish a common approach to online safety.

Communications Policy

Introducing the Online Safety Policy to Pupils

- Online Safety will be taught at the start of each term to cover how to use the internet safely.
- Pupils will be informed that network and internet use will be monitored.
- If the internet is being misused children will be referred to the code of conduct they signed at the start of the year and it be recommended they have technology use suspended for a given time.
- Online Safety lessons will be introduced in Early Years and continued at appropriate levels in Key Stage 2.
- **Staff and the Online Safety Policy**
- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff to receive regular online safety CPD as part of safeguarding training.

Enlisting Parents Support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and the school web site.
- Annual online safety sessions will be scheduled for parents to attend to receive regular updates on keeping their children safe at home using technology.
- The school will take part in annual safer internet week and work to be celebrated/communicated to parents via the newsletter. The computing lead should be in charge of co-ordinating this event.

Appendix 1: Internet Use – Possible Teaching and Learning Activities

Activities	Key E Safety Issues	Relevant
Using search engines to access information from a range of websites	Parental consent should be sought Pupils should be supervised Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with	Web quests e.g <ul style="list-style-type: none"> • CBBC search • Google
Exchanging information with other pupils and asking questions of experts via email	Pupils should only use approved email accounts using the school intranet Pupils should never give out personal information	Purple Mash School Portal.
Publishing pupils' work on school and other websites	Pupil and Parental consent should be sought prior to publication Pupils' full names and other personal information should be omitted	School Website Class Dojo
Publishing images including photographs of pupils	Parental consent for publication of photographs should be sought Photographs should not enable individual pupils to be identified File names should not refer to the pupil by name	School Website Class Dojo
Communicating ideas within chat rooms or online forums	Chat rooms will not be used in school. Only as part of approved blogs/forums. Access to other Social Networking site should be blocked Pupils should never give out personal information	Purple Mash School Portal- Key stage 2 children only
Audio and video conferencing to gather information and share pupil's work	Pupils should be supervised Only sites that are secure and need to be accessed using an email address or protected password should be used	

School Website www.silsoeschool.co.uk

Appendix 2- Code of Conduct (Pupils and Parents)

Dear Parents

RE: Online Safety

At Silsoe Lower School, we prioritise your children's safety online. As part of computing and PSHE across the school, we teach children at their level of understanding how to stay safe when using technology or online. This includes how they should conduct themselves when searching/browsing the internet, understanding the reliability of information online and how to report issues in and out of school. As part of our first lesson back, the children have been learning about E-safety. The children begin the year by signing a code of conduct promising the school they would follow rules to keep themselves and others safe when using technology.

As Silsoe Lower, we understand that e-safety is not just an issue in school but in all areas of a child's life. We emphasise the importance of communication with our trusted adults. We are asking you to co-sign your child's code of conduct to ensure you are aware of our school policies on e-safety and to give your child an opportunity to share what they have learnt in school.

Please return these back to your class teacher as soon as possible.

Thank you for your continued support in keeping our children safe.

Miss Evans
(Computing Lead)

Mrs S Boyle
Head Teacher

Silsoe Lower School Technology Code of Conduct

- I will handle computer equipment carefully
- I will tell an adult in school immediately if I see something that is inappropriate on the computer.
- I will tell an adult in school immediately if I see someone else using technology inappropriately.
- I will use technology appropriately when searching and browsing the internet.
- I understand that if I break these rules I will not be allowed to use technology for an agreed time set by the teacher.
- I will show my values when working on technology.
- I will remember the 3C's (conduct, contact and content) when composing myself on the internet and on technology.

By signing this I _____ accept the computing terms set by Silsoe Lower School to use technology safely and respectfully throughout the year.

Signature: _____

Parent/Carer Signature: _____