WHOLE SCHOOL Online Safety Policy

SILVERDALE ST JOHN'S CE PRIMARY SCHOOL

Inspiring success through learning, community and faith.

I can do all things through Christ who strengthens me – Philippians 4:13

We strive to provide the Christian foundations to enable our children to make good decisions. Our children will be inspired, guided and supported to achieve success, as they are all of infinite worth. Taught through a creative curriculum, our children will become global citizens and will care for all of God's creation.

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).
Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school. community are prepared to deal with the safety challenges that the use of technology brings. The policy is. organised in 4 main sections:
Policies and Practices
Infrastructure and Technology
Education and Training
Standards and Inspection.

2. Silverdale St John's Vision for Online safety

Our school strives to provide a diverse, balanced and relevant approach to the use of Technology, where. children are encouraged to maximise the benefits and opportunities that technology has to offer. Everyone is equipped with the knowledge and skills to safeguard themselves online. This will include:
Learning about the safe use of new technologies.
Recognising and managing potential risks associated online.
Behave responsibly online.

3.The role of the school's Online safety Champion

Our Online safety Champion is Miss Sarah Sanderson.
The roles of the Online safety Champion are as follows:
Having operational responsibility for ensuring the development, maintenance and review of the school's Online safety policy and associated documents, including Online safety agreements. This will be overseen by the Online safety champion, Miss Sarah Sanderson.
Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
Ensuring all staff are aware of reporting procedures and requirements should an Online safety incident. occur.
Ensure the Online safety Incident log is appropriately maintained and regularly reviewed.
Keeping personally up to date with Online safety issues and guidance through liaison with the Local Authority Schools' ICT team and through advice given by national agencies such as the Child. Exploitation and Online Protection Centre (CEOP).
Providing or arranging Online safety advice/training for staff, parents/carers and governors.
Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary.
Liaising closely with the school's Designed Senior person / Child Protection Officer to ensure a coordinated approach across relevant safeguarding areas.

4.Policies and practices

This section of the Online safety Policy sets out the school's approach to Online safety along with the various procedures to be followed in the event of an incident. This Online safety policy should be read in conjunction with the following documentation:

Staff and Governors Online safety agreement.
Parent Online safety agreement.
Pupil Online safety agreement.
ICT Security Framework policy
Behaviour Policy
Whistle blowing policy.

4.1 Security and data management

In line with the requirements of the General Data Protection Regulation (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

• Accurate
• Secure
• Fairly and lawfully processed
• Processed for limited purposes
• Processed in accordance with the data subject's rights
• Adequate, relevant and not excessive
• Kept no longer than is necessary (see privacy notice)
• Only transferred to others with adequate protection.
• All laptops/chromebooks are password protected.
• All children have class or individual passwords and are encouraged not to share it.

All data in the school is kept secure and staff informed of what they can or can't do with data through the Online safety Policy and statements in the Online safety agreements.
The school maps key information that is held.
There is a named person, Mr Ian Gittins with responsibility for managing information.
Relevant staff know the location of data.
All staff with access to personal data understands their legal responsibilities.
The school ensures that data is appropriately managed, both within and outside the school environment, through the use of secure emails.
Staff are aware that they should only use approved means to access, store and dispose of confidential data. Pupil data is kept for 25 years and safely disposed of by the school's Data Protection Officer.
Personal devices, e.g., Smartphone, iPads may not be used to access data on the school system.
Risk of data loss is minimised by having daily back up of the administration networks and weekly back. up for the curriculum network.

4.2 Use of mobile devices

The use of mobile devices offers a range of opportunities to extend children's learning. Staff are aware that. some mobile devices e.g., mobile phones, game consoles or net books can access unfiltered internet content.
These devices are not to be used by pupils in school. Pupils are not allowed to bring mobile phones into school, unless deemed necessary for the purposes of a safe journey to or from school. If a phone is brought in by mistake or for the child's journey to and from school then pupils are asked to hand in the phone to the school office for safe keeping until the end of the day.

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.
To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g., website, brochure or display.

• At school photographs and video of pupils and staff are regarded as personal data in terms of GDPR (2018), and at school we seek written permission for their use from individuals and pupils' parents or carers.
• The school seeks consent from the pupils' parent/carer or member of staff who appears in the media or whose name is used.
• The parental/carer permission is obtained at the beginning of the academic year and is updated on a yearly basis. However, parents have a right to change this during the academic year if deemed necessary.
• The school will not re-use any photographs or videos after staff and pupils have left the school without further consent being sought.

• Parents/carers, who have been invited to attend school events, are allowed to take videos and photographs. We ask the parents not to share these images on social media sites.
• All staff recognise and understands the risks associated with publishing images, particularly in relation to use of personal Social Network sites. It is forbidden for staff to post images or video of pupils taken. at school, in any school activities, on any Social Network sites.
• The school ensures that photographs/videos are only taken using school equipment and only for school purposes.
• The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
• Staff are not allowed to store digital content on personal equipment. Staff are not to use their own. cameras. If used, this will be recorded as a low-level concern.
• When taking photographs/video, staff ensures that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
• Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
• The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the Online safety Champion, S.L.T and Governors on an annual basis.

4.4 Communication technologies
At Silverdale St John's we use a variety of communication technologies and are aware of the benefits and associated risks.
Email
• All staff have access to the Lancashire Grid for learning service as the preferred school email system.
• Only official email addresses are used between staff and with pupils/parents when personal and sensitive data is involved.
• All official emails must not be dealt with using personal equipment e.g., smart phones, iPads etc... All teaching staff are provided with a school laptop to access their email account out of hours.
• The Lancashire Grid for Learning filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
• All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g., Hotmail or Gmail, in school.
• All users are aware that email is covered by GDPR (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
• All users are aware that all email communications may be monitored at any time in accordance with the Online safety agreement.
• Anything being sent by pupils must be authorised by a member of staff.
• All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
• Our school will include a standard disclaimer at the bottom of all outgoing emails (see below).
• Children are able to email using the Google Classroom online system: this only allows them to email each other, or staff members and no-one external to the organization.

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Silverdale St John's CE Primary School. If you are not the intended recipient, you must not use disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that the e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social networks
Social Network sites allow users to be part of a virtual community. Current popular examples of these are. Facebook, Twitter, Tik Tok and Instagram. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other user' content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g., Facebook. minimum age is 13 years old.
All staff are advised that:
• They must not give personal contact details to pupils. Caution should be used when giving personal. contact details to parents including mobile phone telephone numbers, details of any blogs or personal websites.

• Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
• If a social network site is used, details must not be shared with pupils and privacy settings be set at maximum.
• Pupils must not be added as friends on any Social Network site. (See social networking sites and social media policy)
• Adults are aware of the age restrictions for Social Networking sites and have a duty of care to report any known user that is under the minimum age. (See whistleblowing policy)
Remember: whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile phones
• Mobile phones may be used by staff and visitors at appropriate times and only to be used in the staffroom during school hours. Staff and visitors are allowed to use mobile phones in classrooms, out. of hours, when pupils are not present. It is expected that staff and visitor turn their mobile phones on silent during curriculum time. However, in exceptional circumstances prior arrangements can be made with the Headteacher. (See mobile phone policy)
• School has a designated mobile phone for use for school activities e.g., school trips. This is also used for. contact for the After School Care.
• It is acceptable to use personal mobile phones for school activities or in an emergency by prior arrangement by the Headteacher.
• It is not acceptable to use personal mobile phone to support lessons without prior arrangements from the Headteacher.

Instant messaging
Instant Messaging, e.g., WhatsApp, Snapchat, Facebook Messenger, is blocked as default by the school filtering service. If staff wish to use any of these services, either themselves or with pupils, they must apply to the Headteacher for permission. The Headteacher will assess the risk of viewing inappropriate images/making unsuitable contacts in relation to the planned activity before permission is given to access these services. The secure messaging, forum or chat systems within the school's VLE- Google Classroom- will be the preferred way of using instant messaging when appropriate.

Web sites and other online publication
(Including podcasts, videos, 'Making the News' and blogs)
A school website and other online publications e.g., podcasts or blogs, provide an effective way to communicate information. The following statements are what our school deems acceptable and unacceptable use of web sites and other online publication:
• Staff or pupil personal contact information will not be published. The contact details given online will. be the school office.
• The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
• The nominated governor has editorial responsibilities and is responsible for ensuring that content is accurate and appropriate.
• Procedure outlined in section 4.3 (Use of digital media) of this policy will be implemented in the publication of pupil's images, video and work on the school website.
• Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs will be used in preference to than full-face photos of individual children.
• Pupils full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published.
• Work can only be published with the permission of the pupil and parents/carers.
• Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
• The school website will be used to communicate Online safety messages to parents/carers, to provide guidance on the use of digital media.
• Staff and governors are aware what information is appropriate to publish and what information is not appropriate to publish on the school's website.

• The school's website may be edited by nominated staff and a nominated Governor only. Pupils may not edit the website.
• Staff and governors are aware that they may not publish content which is subject to copyright / personal intellectual copyright restrictions.
• Downloadable materials will be in read-only format (e.g., PDF) to prevent content being manipulated and potentially re-distributed without the school's consent.

Video conferencing
• Parents will be asked for permission before pupils take part in video conferencing sessions.
• Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions will be logged including the date, time and the name of the external organisation/person(s) taking part.
• Pupils using video conferencing equipment should be supervised at all times.
• All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'hang up' the call.
• Staff understands that copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.
• Video conferencing will be used to keep in contact with children in the event of a bubble closure, or full lockdown. Staff, children and parents will be made aware of the expectations for ensuring online video conferencing is safe and successful. Zoom and Google Meets will be used for video conferencing.

Others
The school will adapt/update the Online safety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g., Bluetooth and Infrared communication.

4.5 Acceptable Use Policy (AUP)
At Silverdale St John's the Acceptable Use Policy (AUP) is known as the Online safety agreement.
Our Online safety agreement is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.
Online safety agreements (Appendix 1,2,3) are used for Staff and Governors, Visitors and Supply Teachers and pupils must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school.
It is the responsibility of the Online safety champion to make this information available to all staff.
Our school Online safety agreements aim to:
• Be understood by each individual user and relevant to their setting and purpose.
• Be regularly reviewed and updated.
• Be regularly communicated to all users, particularly when changes are made to the Online safety Policy/Online safety agreements.
• Outline acceptable and unacceptable behaviour when using technologies, for example:
o Cyberbullying
o inappropriate use of email, communication technologies and Social Network sites and any online content
o Acceptable behaviour when using school equipment /accessing the school network.

• Outline the ways in which users are protected when using technologies e.g., passwords, virus protection and filtering.
• Provide advice for users on how to report any failings in technical safeguards.
• Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
• Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
• Stress the importance of Online safety education and its practical implementation.
• Highlight the importance of parents/carers reading and discussing the content of the Online safety agreement with their child.

4.6 Dealing with incidents

At Silverdale St John's an incident log is completed to record and monitor offences. All incidents must be reported to the Online safety Champion. This is audited on a regular basis by the Online safety champion and Headteacher.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Potential illegal content must always be reported to the Internet Watch Foundation (http://www.iwf.org.uk). Examples of illegal offences are:
1. Accessing child sexual abuse images
2. Accessing non-photographic child sexual abuse images
3. Accessing criminally obscene adult content
4. Incitement to racial hatred
More details regarding these categories can be found on the IWF website; http://www.iwf.org.uk

• Online safety incidents will be reported to the Online safety champion who will record the incidents into the Online safety Incident log (electronically). The Online safety champion will report all incidents to the Headteacher to discuss appropriate actions to be taken.
• All staff are aware of the different types of Online safety incidents and how to respond appropriately.
• All pupils are informed of procedures through discussions from members of staff.
• Incidents are monitored by the Online safety champion and Headteacher on a regular basis.
• The Headteacher will decide on which point that parents or carers are informed.
• The procedures are in place to protect staff and escalate a suspected incident / allegation involving a staff member

5. Infrastructure and technology
At Silverdale St John's CE Primary School, we ensure that the infrastructure/network is as safe and secure as possible.
We subscribe to the Lancashire Grid for Learning/Lightspeed filter where internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection, but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription, but this needs to be installed on computers in school and then configured to receive regular updates.
We offer the following guidance regarding security:
Pupil access
• All pupils are supervised by staff when accessing school equipment and online materials
Passwords
• All staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at www.lancsngfl.ac.uk/Online safety website.
• All users of the school network have a secure username and password. All pupils have a class username and password whilst all staff have individual usernames and passwords.
• The administrator password for the school network is available to the Headteacher and is kept in a secure place. This is also known by the school IT technician, Richard Prescott and his firm, TechHub.
• Staff and pupils are reminded of the importance of keeping passwords secure.
• All users of the school network are reminded to change their password on a regular basis.
Software/hardware
• The school has legal ownership of all software.
• The school has an up to date record of appropriate licences for all software and the Bursar and IT technician are responsible for maintaining this.
Managing the network and technical support
• Servers, wireless systems and cabling are securely located and physical access restricted.
• The security of the school network is maintained by the ICT Technician.
• The safety and security of the school network is reviewed annually with reference to the guidance provided by Lancashire Schools ICT Centre.
• Computers are regularly updated with software updates/patches as required.
• Staff and pupils have clearly defined access rights to the school's network. Guests such as student

teachers will have the same restricted access rights as the pupils. There is a separate server and secure logins for the school administration computers.
• Staff and pupils are required to log out of a school system when a computer/digital device is left unattended.
• Only the network administrator (i.e. the ICT Technician) is allowed to download executable files or install software.
• Users should report any suspicion or evidence of a breach of security to the Online safety champion or the Headteacher.
• Removable storage devices may not be used in school.
• School equipment including teacher laptops must not be used for personal and family use.
• Personal equipment e.g., iPads, Smartphones, net books etc... must not be used for storing, opening and working on sensitive school data, including images and video of children.
• Staff are made aware that network monitoring/remote access may take place, and this is in accordance with the Data Protection Act 1998.
• External technical support providers (e.g., the ICT Technician) are made aware of the school's Online safety policy.
• The technical support staff are managed overall by the Headteacher and on a week-to-week basis by the ICT Subject Leader.

Filtering and virus protection

• Filtering is provided by the LGfL filtering service, Lightspeed.
• Filtering is managed by the ICT Technician /ICT Subject Leader.
• Filtering service is checked by IT technician and HT monthly and a record of this is kept.
• Virus protection (Sophos) is provided through the LGfL subscription and regularly updated.
• Staff must apply to the Headteacher/IT technician for blocking and unblocking specific websites.
• Staff must report suspected or actual computer virus infection to both the Computing subject leader and the ICT Technician.
• School laptops used at home are set to regularly update virus protection software.

6. Education and training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

6.1 Online safety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own Online safety. Silverdale St John's provides suitable Online safety education to all pupils:
• Regular, planned Online safety teaching is delivered within a range of curriculum areas. A different Online safety thread is the focus of the computing curriculum each half-term.
• Online-Safety education is differentiated for pupils with special educational needs.
• Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues, e.g., using peer mentoring.
• Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
• The school ensures that pupils develop an understanding of the importance of the Online safety agreements and are encouraged to adopt safe and responsible use of ICT both within and outside school.
• Pupils are reminded of safe Internet use e.g. classroom displays, Online safety rules (See Appendices).

6.2 Online safety – Raising staff awareness.

• The Online safety Champion will provide advice / guidance to all members of staff to ensure they are regularly updated on their responsibilities as outlined in this policy.
• The Online safety champion will provide advice/guidance or training to individuals as and when required.
•The Online safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g., use of Social Network sites.
• All staff are expected to promote and model responsible use of ICT and digital resources.
• Online safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online safety Policy and Online safety agreements.
• Regular updates on Online safety Policy, Online safety agreements, curriculum resources and general Online safety issues are discussed in staff / TA meetings.

6.3 Online safety – Raising parents/carers awareness.

“Parents often either underestimate or do not realise how often children and young people come across. potentially harmful and inappropriate material on the internet and are often unsure about what they would. do about it.” (Byron Report, 2008).
Our school offers regular opportunities for parents/carers and the wider community to be informed about Online safety, including the benefits and risks of using various technologies. For example, through the
school’s website, bespoke Parents Online safety Awareness workshop (30.11.21), promotion of external Online safety resources/online materials and the school Facebook page. An Online safety article is included in the school newsletter every half-term.

6.4 Online safety – Raising Governors’ awareness.
Our school considers how Governors, particularly those with specific responsibilities for Online safety, ICT or child protection, are kept up to date. This is through discussion at Governor Meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.
The Online safety Policy will be approved by the governing body and made available on the school’s website. There is a Governor responsible for Online safety who will meet with our Online safety champion on a regular basis.

7. Standards
• The effectiveness of the Online safety policy will be monitored through planning scrutiny, lesson observations, formal conversations with staff and pupils, and monitoring of website access, downloading and email accounts.
• Online safety incidents will be monitored and recorded by the Online safety Champion.
• The introduction of new technologies will be risk assessed and these assessments included in the Online safety policy.
• Any recurring incident will be analysed to see if there is a recurring pattern e.g., specific days, times, classes, groups and individual children.
• Monitoring of Online safety incidents will contribute to changes in policy and practice as necessary. Any changes to policy and practice will be reported to staff and governors through meetings, to pupils by their teacher and to parents via the school newsletter / website.
• Online safety agreements will be annually reviewed and include reference to current trends and new technologies.

This policy was written by Sarah Sanderson in consultation with Mrs Mary Ashton. This policy was reviewed and adapted by Miss Sarah Sanderson (Online safety lead) and Mrs Mary Ashton (Online safety Governors) and approved at the Quality of Education Committee in November 2022.