Silsden Primary School

E-Safeguarding Policy

Young Minds, Free Spirit, Great Future

Silsden
Primary School

Date of Governing Board Approval: September 2020

Review Date: September 2021

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge • Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be reported in the Safeguarding section at committee meetings. The Governor responsible for child protection and e-safeguarding is Lynda Whitton.

The role of this governor will include:

- Safeguarding meetings where e-safeguarding issues will be discussed
- Access to e-safety incident logs – reported to Standards and Pupil Welfare Committee
- reporting to relevant Governors through minutes of the Standards and Pupil Welfare Committee
- Maintaining training and keeping up to date with all online safety issues

Headteacher

- The Head Teacher is the designated E-Safeguarding Coordinator responsible for ensuring the-safeguarding (including e-safety) of members of the school community

. The Headteacher is responsible for ensuring that other relevant staff receive suitable CPD to enable them to carry out their E-safeguarding roles and to train other colleagues, as relevant

- The Headteacher/ E-safeguarding leader is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is detailed in the Safeguarding and Child Protection Policy and the Managing Investigations Procedures adopted by the school.

- takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends the Standards and Pupil Welfare Committee which discusses e-safeguarding issues

. Liaising with the schools curriculum leader to ensure that e-safety teaching and learning is part of our school curriculum.Monitoring all reports that are generated by the schools safeguarding software

Network Manager / Technical staff:

The school receives IT technical support via an external provider there role is to ensure:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that s/he keeps up to date with e-safety technical information and updates the E-safeguarding leader or ICT coordinator as relevant.
- that monitoring software and anti-virus software is implemented and updated

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP- see appendix)
- they report any suspected misuse or problem to the E-Safety leader for investigation
- digital communications with students / pupils (Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities E-safeguarding lessons are taught as necessary across the school year and in particular during the annual e-safety week.

- they continually promote the SMART code for online safety (See Appendix 1)

- students / pupils understand and follow the school e-safety and acceptable use policy
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Children

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign in September before being given access to school systems.

- children are aware that breaking the AUP would cause them to follow sanctions laid out in our Behaviour Policy
- Pupils are encouraged through E-Safeguarding/PSHE lessons to share any E-Safeguarding concerns with a trusted adult

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e-safeguarding. We will assist parents to understand key issues in the following ways:

Regular newsletters offer parents advice on the use of the internet and social media at home.

The SMART Code (see appendix 1) is shared with parents each year during the E Safety Week and parents are encouraged to enforce the code at home.

Acceptable Use agreement for children can be accessed on the website. Parents are asked to discuss these with their child and are invited to sign the forms to say they have done so.

Education

Pupils

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is delivered through the year and in particular during the annual E-Safety Week which takes place in line with the national Safer Internet Day each February
- External E-safeguarding training for pupils on an annual basis
- Key e-safety messages are reinforced as part of the annual e-safety assembly during e-safety week.
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children. Pupils know that any events of Online bullying are taken seriously by the school and they understand the importance of sharing their concerns with a trusted adult.
- Pupils are taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.
- Pupils will sign (age appropriate) the Acceptable Use Policy and a master copy will be on display in the Computing Room.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
-

Staff Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A Staff meeting covering e-safeguarding will take place regularly – at least annually linked to the E Safety Week.
- All new staff should receive e-safety training as part of their child protection induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- All staff will receive a briefing and a copy of the Acceptable use policy annually or as any updated information is made available
- Staff will receive a copy of the E-Safeguarding policy annually or as any updated information is made available, this will also be made available for all through the school's website

Governor Training

Governors take part in e-safety training / awareness sessions

Governors are invited to take part in E-Safeguarding training sessions with staff.

Cyber-Bullying

The sending of unkind, unfriendly or hurtful texts or messages to another child is wrong and constitutes cyber-bullying. The Pupil Acceptable Use Agreement (Appendix 3) makes it clear to children that this is not acceptable. The adults in school will support the child by:

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
  Advising the child not to forward messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our Behaviour policy.

The school may report serious online bullying incidents to the Police. If children receive such messages out of school they are encouraged to report it to an adult in school so the school can investigate and respond.

Internet Provision

The school Internet is provided by Schools Broadband. All sites are filtered using the providers filtering system which also generates reports on user activity.

The school subscribes to the e-safe monitoring system. This system monitors all computing usage in school and provide the e-safety leader with weekly monitoring reports highlighting any inappropriate usage.

Managing ICT systems and access

Access to ICT systems is managed by the external IT Support provider.

All children at the school receive logins and accounts. These accounts are managed through administrator privileges which are only known to the Technician and Coordinator. Accounts are created for new starters at the beginning of the academic year and then for new starters that join during the school year. Accounts are deleted annually for any leavers including those children in year 6.

Adult are given accounts for school systems. Adults are given accounts for school systems. Accounts are created and deleted for new starters and leavers when required.

Passwords

All users (staff and pupils) have the responsibility for the security of their user name and password and must not allow other users to access the systems using their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported to the E-Safeguarding Coordinator.

- Passwords for new users and replacement (passwords for existing users can be allocated by the external IT Support provider.)
- Members of staff are made aware of the school's password rules through induction, the Acceptable Use Policy and the E-Safeguarding policy.
  Pupils are made aware of the school's password rules through Computing/E-Safety lessons and through the Pupil Acceptable Use Policy.
- Old user names and accounts are deleted annually.

All KS1 and KS2 pupils have their own individual log in and password for accessing the school's ICT systems. EYFS pupils have generic passwords when logging in to the schools systems.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online.
- Staff are allowed to take digital / video images to support educational aims. Those images should **only** be taken on **school equipment**; the personal equipment of staff should not be used for such purposes.

- Parents or carers must give express consent for photographs of students / pupils to be published on school publications, website, blog or press (see form in appendix)

Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Do not transfer data using devices such as memory sticks, unless approved by the Headteacher and using a school encrypted device. The use of home bought devices is forbidden.

Social Media

Silsden Primary School uses twitter and a website to communicate to external parties. These are secure and can only be updated and changed by designated users in school.

All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school.

Mobile phones - Pupils

Pupils are not permitted to have mobile phones at school. In exceptional circumstances, children may need a mobile phone before or after school. If this is the case, the phone should be handed in at the School Office directly on arrival at school. The School Administrator will label the phone and lock away for the day. The phone should be collected at the end of the day. The phone should not be used on the school grounds except in exceptional circumstances under the supervision of a senior leader. The school takes no responsibility for lost, stolen or damaged mobile phones.

School mobile devices

The school has a variety of mobile devices including iPads, note-books and Laptops. All of the statements included in the Acceptable Use Policy apply to these mobile devices. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children however some devices operate on generic logins so the individual cannot always be identified.

Acceptable Use Policies for staff and pupils are included in the appendices of this policy.

Development and Review of this policy

Monitoring of the policy will take place annually, or more regularly in light of any significant new developments in the use of technologies, new threats to E-Safety of incidents that have taken place.

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. (Regulation of Investigatory Powers Act 2000).

Policy Date: September 2020 Review Date: September 2021

This policy has been approved and adopted by the Governing Body.

Signed ..... (Chair of Governors) Date.....

Appendix 1:

We promote the SMART rules from www.kidsmart.org.uk and www.childnet.com

Safe: *Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.*

Meeting: *Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.*

Accepting: *Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!*

Reliable: *Information you find on the internet may not be true, or someone online may be lying about who they are.*

Tell: *Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.*

Appendix 2:

Silsden Primary School

IT Acceptable Use Agreement for Staff

This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of technology. Technology relates to ICT systems, hardware, software, internet, email, mobile devices, cameras, laptops and memory devices.

Members of staff:

- Must only use the school's technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. It is a criminal offence to use an ICT system for uses other than those permitted by its owner.
- Must only use approved, secure school email systems for any school business.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.
- Have a duty to protect their passwords and personal network logins, and should log off the network when leaving a workstation unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- Must not install any software or hardware without permission from a technician or the ICT coordinator.
- Are not permitted to use personal devices or portable media for storage of school related data/images (e.g. USB stick) without encryption and the express permission of the Headteacher.
- Should ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely.
- May only use school equipment to post pictures to the website or Twitter.
- With the written consent of parents and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Should ensure that their use of social networking sites, such as Facebook, Twitter and Instagram, does not question or bring their professional role into disrepute. Members of staff:
  - Are advised to consider, and set appropriately, their privacy settings on such sites.
  - Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
  - Should not communicate with pupils, in relation to either school or non-school business, via social media. Members of staff should only communicate with pupils using the appropriate systems approved by the Headteacher. Staff should at all times follow the school's Social Media and ICT Policy.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.

- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.
- Must promote and model positive use of current and new technologies and e-safety.
- Must respect and comply with copyright and intellectual property rights.
- Have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to the Headteacher.

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in the line with the School's Disciplinary Procedure.

I have also read and understood the Staff Code of Conduct and the Silsden Primary School Social Media and IT Policy

Signature: …… Date: ……..

Full Name ……..…… Job Title: ……

Appendix 3:

Silsden Primary School

Pupil Acceptable Use of ICT in School Agreement

- We only access the computer system with the login and password we have been given
- We don't access other people's files or use their password and login details
- We ask permission before using the Internet
- We immediately hide any webpage we don't like and inform a teacher
- We only email people our teacher has approved
- We send emails that are polite and friendly
- We never use the internet, email or texts to send unfriendly, unkind or hurtful messages. This is cyberbullying.
- We will immediately report any unpleasant messages received as this would help protect other children and ourselves
- We never give out a home address, phone number, passwords or other personal information.
- We never arrange to meet anyone we have met over the Internet
- We never open emails sent by people we don't know
- We tell the teacher if we see anything on a device we are unhappy with
- We will not alter the settings on any device without the permission of the teacher
- We will not download any software or programs on to a device without the permission of the teacher.

- We understand that we are responsible for good behaviour on the Internet and when using ICT equipment, inappropriate use may lead to access being withdrawn

Signed: Date: