SKERTON
ST LUKE'S
CE VA PRIMARY SCHOOL

Live, Learn, Thrive
Love God, love each other

POLICY FOR
ONLINE SAFEGUARDING

Reviewed: September 2024
Review Due: Autumn 2025

School Christian Values

Generosity, compassion, courage, forgiveness, friendship, respect, Thankfulness, trust, perseverance, justice, service and truthfulness.

Bible Reference

Luke 10: 27 'Love the Lord you God with all your heart, with all your soul, with all your strength and with all your mind. Love your neighbour as yourself'

Policy References

This policy is written with reference to the following school policies:

- Single Equalities Policy.
- Inclusion Policy
- SEND
- KCSIE
- Positive Behaviour Policy
- Communication Policy
- Complaints Procedures
- Attendance Policy

Most of these policies are available on the school website. In addition, copies of the following policies are available, on request, from the school office.

Contents

Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment. Pupils are growing up in a world where they are in living their lives seamlessly online and offline.

Information and Communications Technology (Computing) covers a wide range of resources including; web-based and mobile and, on occasion, remote learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Our whole school approach at Skerton St Luke's CE Primary School, we are preparing children to make the best use of the internet and technology in a safe, considered and respectful way. Currently the internet technologies children and young people are using both inside and outside of the classroom include, but are not limited to; websites, apps, learning platforms, virtual learning environments, email and instant messaging, social networking, streaming of TV, music and videos, media including social, news and advertising, blogs, vlogs and podcasts, gaming, mobile and smart technologies like phones and watches with text, video and/or web functionality.

Whilst exciting and beneficial both in and out of the context of education, many areas of accessing technology, 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 Skerton St Luke's Primary School, we understand the responsibility to educate our pupils in online safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Intent

1. Enhance their natural curiosity by giving them access to a wide variety of information in different contexts through a progressive sequence of work.
2. Solve problems in today's digital world and discuss their learning and thought process to talk about their learning fluently with correct technical vocabulary.
3. Become confident, familiar and proficient in using a variety of computing equipment both in school and the outside world.
4. To connect with others safely, positively and respectfully through different hardware, software and media.
5. To understand the effects of their own online actions on others and knowing how to display and recognise respectful behaviour online.
6. To navigate the online world safely and confidently regardless of device, app or platform.

Key Roles

Computing subject leader:

- Promote the importance of online safety throughout all teaching and learning with technology
- Share regular information and deliver training on online safety issues
- Attend and implement training from external sources e.g. Local Authority
- Write, update and implement policies for Computing.
- Support implementation of new curriculum, software, hardware and policies
- Design school's internet access expressly for pupil use and will include filtering systems (Smoothwall) appropriate to the age of pupils that are regularly monitored

DSL:

- Share regular information and deliver training on online safety issues.
- Attend and implement training from external sources e.g. Local Authority
- Write, update and implement policies for Online Safety and Acceptable Use (appendix 1)
- Alongside technical support and DSLs, monitor technological usage
- Support actions related to online safety concerns alongside Safeguarding Team

Governors:

- Foster and embed a high profile of online safety throughout school which is maintained by all staff
- Monitor the implementation of new curriculum, software, hardware and policies
- Have a designated governor to support the teaching of computing
- Designate a member of staff to lead computing

Staff:

- All staff will be provided with online safety information and training at induction.
- All staff will be provided with CPD-accredited online safety training:
- L1 Online safety training for non-teaching staff and parents/carers
- L2 Online safety training for Governors and teaching staff
- L3 Online safety training for DSLs, Computing Lead and SENDCOs.
- Promote and maintain high visibility for online safety
- Embed online safety teaching throughout all teaching with technology
- Receive regular information and training on online safety issues
- Online Safety training as part of induction of new staff
- Read, understand, sign and apply the Acceptable Use agreement (appendix 1)
- Request training where there is a lack of knowledge or support needed
- Deliver a broad and balanced curriculum with full coverage
- Monitor pupils' usage of technology when teaching
- Report any concerns of breach of online safety (appendix 2) to Safeguarding Team and log on CPOMS under 'Online Safety' category
- Following advice from the safeguarding team, where issues relate to individual children, inform parents that day of any concerns
- Make sure that all copyright laws are adhered to in materials used in the classroom and published publically, e.g. on the school website
- Communicate with external agencies appropriately e.g. e-mail sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper.

Parents:

- Provided with up-to-date CPD resources that covers all aspects of online safety. This includes a weekly online safety link to Wake Up Wednesdays from National Online Safety and access to informative webinars.
- Discuss with children the Acceptable Use agreement and its importance
- Support the Online Safety policy and its intent
- Report any concerns of online safety to a teacher or trusted adult in school
- Follow online safety rules outlined in Acceptable Use agreement when completing remote learning out of school
- Keep up to date with school's information through the provision of newsletters, school website, Parent App and assemblies.

Pupils:

- Use all computing equipment as outlined by staff in the lesson
- Read, understand, sign and apply the Acceptable Use agreement
- Follow online safety rules outlined in Acceptable Use agreement when in school
- Follow online safety rules outlined in Acceptable Use agreement when completing remote learning out of school
- Report any concerns of online safety to a teacher or trusted adult in school
- The school council to promote online safety and attend meetings to discuss ongoing issues

Teaching Online Safety

To allow a comprehensive curriculum to teach online safety and reach the intent for this policy, Skerton St Luke's CE Primary school has taken advice from Teaching Online Safety in schools, DFE, June 2019. As outlined in this document, Skerton St Luke's has used National Curriculum objectives (Appendix 3) and Education for a Connected World (Appendix 4) as a basis for teaching online safety. This allows for a broad and balanced curriculum that not only links to the teaching of computing, but PSHE and other curriculum areas to allow for children to be prepared for a life with forever progressing technology. As well as this formal teaching, educating pupils on the dangers of technologies that may be encountered outside of school is also done informally when opportunities arise. To make sure that all children are safeguarded and taught about online safety, our teaching begins with age-appropriate units from EYFS through to the end of KS2.

Key Questions underpinning teaching of online safety:

- How do you recognise techniques used for persuasion?
- How can you effectively evaluate what you see online?
- What is acceptable and respectful online behaviour?
- How do you identify online risks?
- How and when do you seek support?

Pupils are taught

- How to recognise when to seek advice or help if they experience problems when using the internet and related technologies who to report a concern to; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The impact of online bullying on others
- What to do in response to being bullied online
- Effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- How to communicate effectively using technology e.g. email and message
- What information is safe to share and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.

As per the Keeping Children Safe in Education, 2023, guidance, whilst the breadth of issues classified within online safety is considerable and ever-evolving, they can be categorised into four areas of risk; content, contact, conduct and commerce.

This can be classified to a child as:

- engages with and/or is exposed to potentially harmful CONTENT;

- experiences and/or is targeted by potentially harmful CONTACT;
- witnesses, participates in and/or is a victim of potentially harmful CONDUCT;
- is party to and/or exploited by a potentially harmful CONTRACT.

Content Risks

Content risks are among the main risks to children online, which is most commonly exposure to harmful content or that which is unsafe for children. Examples include exposure to profanity, sexual content or nudity, highly violent or otherwise gory and disturbing content, and animal cruelty.

Contact Risks

Contact risks refer to the communication with people who have hidden agendas or are 'actors' that can cause harm to children. These actors may include child predators, fraudsters, criminals, terrorists, or adults pretending to be children.

Conduct Risks

Conduct risks are the risks of children participating in behaviours that may be harmful, either physically or emotionally. These include bullying, dangerous behaviours such as self-harm activities, dangerous viral challenges, radicalisation, or encouragement of eating disorders.

Contract Risks

Contract risks involve the risk of children agreeing to terms or contracts they don't agree with or understand. These may include signing up to receive inappropriate marketing messages, inadvertently purchasing something, or providing access to personal data.

It is also important to note that although these risks have been classified into four areas, it is common that a risk may be more than one area at once and more complex than being separate and clear cut into just one.

Units of Work

The teaching of online safety is broken up into 8 different units (appendix 4):

1. Self-image and identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, well-being and lifestyle
7. Privacy and Security
8. Copyright and ownership

For more detail about what children are taught in each unit of online safety, please see the Computing Policy

Monitoring, Filtering and Management

To ensure that Skerton St Luke's CE Primary School has a commitment to safeguarding children online, we have updated our filtering and monitoring procedures.

As part of our safeguarding duty, it is our responsibility to ensure there are appropriate measures in place to limit children's exposure to risks such as potentially harmful or inappropriate online content through the IT system. Whilst we cannot ensure 100% effectiveness of this, we have a number of measures to ensure that it is limited as best we can to ensure safeguarding.

Our filtering and monitoring system does not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

To ensure that filtering and monitoring is in place and reviewed regularly, Headteacher [Catherine Armistead], Computing subject leader [Sophie Beatty], deputy DSLs [Helen Walling-Lewis and Rachel Stephenson] and school technician [Jez Rey] will work together to ensure that the appropriate policy is followed as outlined here. This will then be overseen by safeguarding governor [Jude Gault]. This information will also be given to staff through annual safeguarding training updates, or more frequently should the need arise.

Filtering is the availability or extent to which, content is contextually filtered. This can also include where remote devices are able to receive school based filtering. At Skerton St Luke's CE School, we use Smoothwall to ensure filtering. The virus protection is updated daily and overseen by technician Jez Rey. Where there is the discussion for blocking or unblocking content, this will be discussed with the team as detailed above. It is sometimes important to take into account the context of content, e.g. historical events, which may be usually blocked but relevant to a unit of learning for a teacher to access.

Within this review, it will include:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

When recording the checks, it will be logged:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

Prior to children joining school, an internet usage will be included and required to be signed following discussion with the child by the parent/carer. Where children are using devices, they will need to login to access the internet. EYFS, Year 1 and Year 2 will use a class log in. Year 3, 4, 5 and 6 will use individual logins. Through the teaching of online safety within both Computing and PSHE curriculums, children will be taught the importance of not sharing passwords and effective password creation.

Monitoring is the capability or extent to which remote devices are monitored by technology monitoring services and then analysed. This can include the expansion on the presentation of internet logfile information or the physical location of monitoring data.

There are three types of monitoring:

1. Physical monitoring
    - It is set out that all children are supervised when using devices that have the capability to connect to the internet. It is the expectation that such devices are only used for educational based activity as directed by the teacher as part of the curriculum.
2. Internet and Web Access
    - As detailed above in filtering, there are daily updated to services, review of blocked sites and a team in place to analyses and review the access to the internet. It must also review content in multi-lingual sites.
3. Active Monitoring

- At Skerton St Luke's CE School, we use Smoothwall Monitor Managed service which sends automatic alerts to identified DSLs. This will give information as to the event type, the username, date, time and message/concern. This is then followed up as per the Safeguarding policy where actions and intervention can be taken, and further teaching points can arise.

Where there are concerns that are regarding children's access to the internet, the safeguarding policy is to be followed. Report immediately to a DSL, follow actions as directed, record concerns on CPOMS.

Internet Access

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.

- Children must sign in to access the internet. This allows each child to be monitored by the school technician, Jez Rey, who will be alerted should a concern arise.
- EYFS, Year 1 and Year 2 use a class login
- Year 3, Year 4, Year 5 and Year 6 use individual children's logins
- Virus protection will be updated daily.
- Security strategies will be discussed regularly between senior management with the computing subject leader and fed back to staff where needed.
- Staff or children must not share logins to internet or other software
- The school will work with the LA, DfE and the Smoothwall Support Team, and computing cluster meetings to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, computing subject leader (Mrs Beatty) school technician (Jez Rey) or Headteacher (Mrs Armistead) or Mrs Walling-Lewis (DSL) or other Designated Safeguarding Lead.
- The school technician will ensure that the filtering methods selected are appropriate, effective and reasonable. Any issues will be reported to the safeguarding team.
- The school technician will monitor technology accessing both the internet and network logins and usage
- The school technician will monitor the usage of the school website

Internet and Network Usage

- Written permission from parents must be obtained to use the internet and network access
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Children will only use technology and the internet for educational purposes as directed by a teacher or staff member.
- Children will only be able to access their class folder on computer and use their own logins for software e.g. TT Rockstars, Purple Mash
- Mobile phones/smart watches brought to school by pupils must be kept in the school office. Staff will use a school phone where contact with pupils/parents is required.
- Staff should not use personal mobile phones/smart watches or other communication devices during the school day except during breaks in the staff room. These devices should be connected to the school's Wi-Fi.
- Pupils may only use approved accounts on the school system including email, messaging and software logins

- The school technician, Jez Rey, will give permission for staff technology (e.g. laptops) to use the school network and internet
- Staff to use a school email for any professional contact to colleagues or external agencies
- Children must only access the internet when instructed by an adult

Protecting personal data

We will ensure that all personal information supplied is held securely, as defined by the GDPR. Parents and children have the right to view the personal information that the school holds about them/their child and to have any inaccuracies corrected. (except information where this contradicts safeguarding children legislation). Staff must make sure that all data held by staff is secure and that if data is being taken offsite, e.g. portable hard drives, either the sensitive data or device itself is encrypted and password protected.

For more information on GDPR, please see the GDPR policy.

Reporting a Concern (appendix 2)

- Complaints of internet misuse will be dealt with by a member of the safeguarding team or SLT. Page
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection or safeguarding nature must be dealt with in accordance with school child protection procedures and reported to the DSL. For more information on these procedures, please see the Safeguarding and Child Protection policy.

Published Content including Media

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 headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work at Skerton St Luke's CE School

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or external media e.g. social media, local press etc. (see appendix 5)
- Permissions will be updated as required:
  - Every 5 years (on entry to school and in Year 3)
  - New entry to school
  - Update or change to policy or legislation
- Parents/carers may withdraw permission, in writing, at any time but with the conversation that whilst we can remove any previous media available to us, it is not possible to remove it from the internet entirely.
- Photographs that include pupils will be selected carefully and full names will not be used in association with photographs.
- Individual pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, e.g. school performances and assemblies etc. the school will demonstrate our protective ethos by announcing that photographs may only be taken of children whose parents are present at the time and they are for private retention and not for publication in any manner, including use on personal websites or social media

Social networking and personal publishing

For more information about staff use, please see the Use of Social Networking Sites and Social Media Policy.

- The school will block/filter access to social networking sites but children will be taught safe use of these through the online safety curriculum.
- Pupils and parents will be advised that the use of social network spaces outside school without supervision is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be taught about their internet footprint and how to Page 12 of 26 access these safely. They will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised through assemblies, computing sessions, PSHE lessons and ongoing class discussion to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Parents are reminded about online safety through the school website, newsletters and at information evenings.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff are NOT permitted to add children or family members as 'friends' if they use these social media sites. If there is an instance where a staff member is linked with a parent on social media, this is to be declared and discussed with the head teacher.

Supporting Vulnerable Pupils

There are some pupils (looked after, CP, CIN, SEND) who are more susceptible to online harm or who have less support from home in staying safe online. Support included in the offer for these pupils is:

- Additional support offered at Parents' Evening to discuss online safety
- Advice through PEP, Core Group or Multi-Agency Meetings to support parents or carers with keeping children safe online
- Support to parents and carers with the appropriate questions and conversations to have with children
- Additional support on the website to guide parents to external advice e.g. Digital Parenting Magazine, Parent Zone, NSPCC etc.
- Guidance with what is acceptable behaviour and supporting children with being independent in regulating their own usage of technology and knowing when and how to seek help, advice or support

Remote Learning

For more information, please see the Remote Learning policy and the Safeguarding and Child Protection policy.

In some instances, children may need to learn from home. It is important that all staff who interact with children, including online, continue to look out for signs that a child may be at risk. Any such concerns should be dealt with as per the Safeguarding and Child Protection policy. If required following reporting to a DSL, referrals should still be made to children's social care and as required, the police.

Adults in school **under no circumstances** should contact via phone, email or social media children or families on a personal account or device. If families need to be contacted, use a school phone or ask a member of SLT or DSL for advice on contacting via email or other means. If a member of staff is contacted by a child or child's family member via a personal account of device, this should be reported to a DSL and further advice taken. School designated 'homework'

emails should be used by teachers for correspondence with parents, that are then monitored by SLT. Work should be set via the Remote Learning Policy using agreed systems e.g. Class Dojo.

Any use of online learning tools and systems need to be taken into account alongside GDPR and data protection requirements. Any live teaching that takes place, must have two adults present, the host and a member of SLT. **Under no circumstances** must 1:1 live teaching or meetings take place. All staff should follow guidance from SLT on home learning and follow a consistent approach.

If completing a live meeting or teaching the following must be adhered to:

- No 1:1s, groups only
- A member of SLT should be present so there are two members of staff during the whole meeting/teaching
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Cameras of participants should be off to an external audience
- Only first names to be used
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held.

We recognise that school is a protective factor for children and young people, and the current circumstances can affect the mental health of pupils and families. Teachers need to be aware of this in setting expectations of pupils' work where they are at home.

On occasion, families may need to borrow equipment when learning at home. An adult with parental responsibility must sign the Equipment Home Loan Agreement – Child (Appendix 6) on behalf of the pupil. If an adult is borrowing equipment for their own use (e.g. parental learning courses) then the adult must read and sign the Equipment Home Loan Agreement – Parent (Appendix 7).

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by Mrs Armistead (Headteacher) alongside computing subject leader Mrs Beatty. This policy is the governors' responsibility and they will review its effectiveness regularly.

Reviews will take place termly with Computing subject leader – Mrs Beatty, Designated Safeguarding Lead, Mrs Armistead and governor with responsibility for computing, Mr Greenwood and governor with responsibility for Child Protection, Mrs Gault.

Reviews will then be reported to the full governing body. Ongoing incidents will be reported to the full governing body.

Appendix 1 – Acceptable Use Agreement

KS1 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

1. I will only use the school's ICT equipment for schoolwork. If I need to use the school's computers for anything else, I will ask for permission from a member of staff.
2. I will not share my passwords with other people and will tell my class teacher if I think someone else knows them.
3. I will not share personal details about myself such as name, phone number or home address on email or social media.
4. I will make sure that all my contact with others using computing equipment is respectful, positive and polite.
5. If I see something on a screen that upsets me or is inappropriate, I will always tell a trusted adult.
6. I will gain permission from peers of adults before taking photos of them.
7. I know that my use of computing equipment can be checked and my parent or carer can be contact if school is concerned for my safety.
8. I know that these rules are here to keep me safe.

I have read and understood these rules and agree to them.

Signed: _____

Date: _____

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

1. I will only use the school's computers for schoolwork. If I need to use the school's computers for anything else, I will ask for permission from a member of staff.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will gain permission from my peers or adults before taking photos of them.
4. I will not share my logins or passwords.
5. I am aware that some websites and social networks have age restrictions and I agree to abide with these age restrictions in school.
6. I will not attempt to visit internet sites that I have not been instructed to.
7. I will make sure that all my contact with others using computing equipment is respectful, positive and polite.
8. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
9. I will not give any personal information (home address, phone number, photographs & videos) that could be used to identify me on any website, social media or messaging.
10. I will never arrange to meet someone I have only ever previously met through the internet.
11. If I see something on a screen that upsets me or is inappropriate, I will always tell a trusted adult.
12. I know that my use of computing equipment can be checked and my parent or carer can be contact if school is concerned for my safety.
13. I know that these rules are here to keep me safe.

I have read and understood these rules and agree to them.

Signed: _____

Date: _____

Sandylands Staff Acceptable Technology Use Policy (AUP)

For more information about staff use, please see the Use of Social Networking Sites and Social Media Policy.

1. I will only use the Skerton St Luke's Primary School digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by Skerton St Luke's Primary School.
2. I will not reveal my password(s) to anyone.
3. I will not engage in any online activity that may compromise my professional responsibilities.
4. I will only use the approved communication systems with young people, parents/carers, and I will only communicate with them on appropriate Skerton St Luke's Primary School business.
5. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to Catherine Armistead (Headteacher - Designated Safeguarding Lead).
6. I will not download any software or resources from the internet that can compromise my school computer, or are not adequately licensed.
7. I will not use personal digital cameras or camera phones for taking and transferring images of young people and will not store images at home.
8. I agree and accept that any computer, laptop, other devices loaned to me by Skerton St Luke's Primary School, is provided solely to support my professional responsibilities and must be returned.
9. I understand that GDPR requires that any information seen by me with regard to young people's information will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
10. I will embed the online safety ethos for adults and young people into my area of work.
11. I understand that all internet usage may be monitored and logged and this information could be made available to a senior member of staff on request.
12. I understand that failure to comply with this agreement could lead to disciplinary action.
13. I will not use my personal electronic communication devises e.g. mobile phone, tablets, smart watches (or any other device with access to the internet or networks) during the school day except during breaks and always in the staff room.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand Skerton St Luke's Primary School's most recent online safety policies.

Signature _____

Date _____

Full Name _____ (printed)