Southridge First School

Online (E-Safety) Policy

This policy was reviewed and approved by the Curriculum Committee on 9th October 2018 and adopted by FGB at the Autumn term meeting (2018)

Review Date: Autumn 2019

Online Safety (E–Safety) Policy for Southridge First School

Contents

How to use this document

1. Creating an online safety ethos
    - 1.1. Aims and policy scope
    - 1.2. Writing and reviewing the online safety policy
    - 1.3. Key responsibilities of the community
        - 1.3.1. Key responsibilities of the management team
        - 1.3.2. Key responsibilities of the online safety/designated safeguarding lead
        - 1.3.3. Key responsibilities of staff
        - 1.3.4. Additional responsibilities of staff managing the technical environment
        - 1.3.5. Key responsibilities of children and young people
        - 1.3.6. Key responsibilities of parents/carers
2. Online communication and safer use of technology
    - 2.1. Managing the website
    - 2.2. Publishing images online
    - 2.3. Managing email
    - 2.4. Appropriate safe classroom use of the internet and associated devices
    - 2.5. Management of school learning platforms/portals/gateways
3. Social media policy
    - 3.1. General social media use
    - 3.2. Staff personal use of social media
    - 3.3. Pupil use of social media
4. Use of personal devices and mobile phones
    - 4.1. Rationale regarding personal devices and mobile phones
    - 4.2. Expectations for safe use of personal devices and mobile phones

4.3. Children use of personal devices and mobile phones

4.4. Staff use of personal devices and mobile phones

4.5. Visitors use of personal devices and mobile phones

5. Policy decisions

5.1.Recognising online risks

5.2. Internet use within the community

5.3. Authorising internet access

6. Engagement approaches

6.1.Engagement of children and young people

6.2. Engagement of children and young people who are considered to be vulnerable

6.3. Engagement of staff

6.4. Engagement of parents/carers

7. Managing information systems

7.1.Managing personal data online

7.2. Security and managing information systems

7.3. Filtering decisions

7.4. Management of applications to record progress

8. Responding to online incidents and concerns

Appendix A: Procedures for responding to specific online incidents or concerns (including, online child sexual abuse, indecent image of children, radicalisation and cyberbullying)

Appendix B: Notes on the legal framework

Appendix C: Online safety contacts and references

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

Southridge First School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
Southridge First School identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
Southridge First School has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools management functions. Southridge First School also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

The purpose of Southridge First School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Southridge First School is a safe and secure environment.
- Safeguard and protect all members of Southridge First School community online.
- Raise awareness with all members of Southridge First School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.
This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE).

1.2 Writing and reviewing the online safety policy

1.2

Southridge First School online safety policy has been written by the school, involving staff, pupils and governors, building on the Kent County Council online safety policy template with specialist advice and input as required.

The policy has been approved and agreed by the Leadership Team and governing body.

The schools online safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.

The School Online safety (e-Safety) Coordinator is Mr F. Willcock

The School Designated Safeguarding Lead (DSL) is Mr F Willcock and Deputy Designated Safeguarding Lead (DpSL) is Mrs Hall

The School Online safety (e-Safety) lead for the Governing Body is Mr I. Selkirk

Policy approved by the Curriculum Committee: Date: 9th October 2018

Policy approved by Governing Body: Date: Autumn 2018

The date for the next policy review is Autumn 2019

1.3 Key responsibilities of the community

1.3.1 Key responsibilities of the school and governing body are:

Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
Supporting the online safety (e-Safety) lead in the development of an online safety culture within the setting.
Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
Making appropriate resources available to support the development of an online safety culture.
Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
To work with and support technical staff in monitoring the safety and security of schools systems and networks.
To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
To ensure that the Designated Safeguarding Lead (DSL) works in partnership with the online safety (e-Safety lead and ICT support person complies with all recommendations outlined in the policy.

1.3.2 Key responsibilities of the designated safeguarding/online safety lead are:

Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
Keeping up-to-date with current research, legislation and trends.
Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day with responsibility delegated to the ICT lead to facilitate
Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches, assisted by the ICT lead person in school
Work with the school/setting lead for data protection and data security to ensure that practice is in line with legislation.
Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
Monitor the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
Liaising with the local authority and other local and national bodies as appropriate.
Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input. In collaboration with ICT lead in school.
Ensuring that online safety is integrated with other appropriate school policies and procedures.

Meet regularly with the governor/board/committee member with a lead responsibility for online safety

1.3.3 Key responsibilities of staff are:

Contributing to the development of online safety policies.
Reading the school Acceptable Use Policies (AUPs) and adhering to them.
Taking responsibility for the security of school/setting systems and data.
Having an awareness of online safety issues, and how they relate to the children in their care.
Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
Embedding online safety education in curriculum delivery wherever possible.
Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
Knowing when and how to escalate online safety issues, internally and externally.
Being able to signpost to appropriate support available for online safety issues, internally and externally.
Maintaining a professional level of conduct in their personal use of technology, both on and off site.
Taking personal responsibility for professional development in this area.

1.3.5. Additional responsibilities for staff managing the technical environment are:

Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 Key responsibilities of children and young people are:

Contributing to the development of online safety policies.
Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
Respecting the feelings and rights of others both on and offline.
Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

Taking responsibility for keeping themselves and others safe online.
Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6. Key responsibilities of parents and carers are:

Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
Role modelling safe and appropriate uses of new and emerging technology.
Identifying changes in behaviour that could indicate that their child is at risk of harm online.
Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

2.1

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
Pupils work will only be published with their permission or that of their parents/carers.
The administrator account for the school website will be safeguarded with an appropriately strong password. Access will only be to designated key people in school.
The school will post information about safeguarding, including online safety on the school website.

2.2 Publishing images online

2.2

The school will ensure that all images are used in accordance with the parental permissions given. Written permission from parents or carers will always be obtained before images of pupils are electronically published e.g. website, learning platform, newspapers.

2.3 Managing email

2.3

Pupils may only use school/setting provided email accounts for educational purposes.
All members of staff, including governors, are provided with a specific school/setting email address to use for any official communication.
The use of personal email addresses by staff for any official school/setting business is not permitted.
The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.

Sensitive or personal information will only be shared via email in accordance with data protection legislation.
Governors should use SMT and teacher contact emails for governor business only. Other correspondence should follow school guidelines for all parents for transparency and equal access.
All parent enquiries should come through Southridge email. Staff responses need to be returned in the same way, not through personal accounts. However, we recognise that in Reception and Nursery parents contribute to their child's learning journey via ntlp email direct with the staff.
Access in school to external personal email accounts may be blocked.
Excessive social email use can interfere with learning and will be restricted.
Email sent to external organisations should be written carefully and **authorised** before sending, in the **same way** as a letter written on **school headed paper** would be. Any references requested should always be sent via North Tyneside email and authorised by Headteacher or Deputy Head.
School email addresses and other official contact details will not be used for setting up personal social media accounts.
School email accounts should be checked regularly during working days. Personal use of emails is restricted to outside school working hours unless approved by SMT.

2.4 Appropriate and safe classroom use of the internet and associated devices

2.4

The school's internet access will be designed to enhance and extend education.
Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
Pupils will use age and ability appropriate tools to search the Internet for content.
Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
Supervision of pupils will be appropriate to their age and ability
At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

Pupils will only use computers when a teacher or TA is in the room. No access is available at lunch time or break unless the conditions above apply.
All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place. All ipads will be locked away when not in use, have secure access codes and signed in and out so they may be located. Permission needs to be given to take them off site from Headteacher or Deputy Head. No images are to be downloaded onto any device out of school.
All school laptops must be onsite during the school day and accessible if needed in school. During school holidays and weekends they may be kept at home in a safe and secure place, covered by staff home insurance and securely password protected. Any loss or damage will be the responsibility of the member of staff and must be reported immediately to the Headteacher or deputy. Laptops must only be used for school use, including internet searches. School staff only are permitted to use them.
Where an employer finishes work at the school, the ipads, computers or cameras must be returned to school on the last teaching day. The device is only to be cleared and checked by ICT services.
Images of pupils or documents containing names should not be stored on laptops, only on the school server, unless approval is granted.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.
Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

2.5 Management of school learning platforms/portals/gateways

2.5

SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
Pupils/staff will be advised about acceptable conduct and use when using the LP.
Only members of the current pupil, parent/carers and staff community will have access to the LP.
All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
Any concerns about content on the LP may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LP for the user may be suspended.
d) The user will need to discuss the issues with a member of leadership before reinstatement. e) A pupil's parent/carer may be informed.

A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1. General social media use

3.1.

Expectations regarding safe and responsible use of social media will apply to all members of Southridge First School community and exist in order to safeguard both the school and the wider community, on and offline.
All members of Southridge First School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Southridge First School community.
All members of Southridge First School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
The school will control pupils and staff access to social media and social networking sites whilst on site and using school provided devices and systems.
The use of social networking applications during school hours for personal is not permitted.
Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
Any concerns regarding the online conduct of any member of Southridge First School community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Staff personal use of social media

3.2

Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
All members of staff are advised not to communicate with or add as 'friends' any current or past pupils.
If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
All communication between staff and members of the school community on school business will take place via official approved communication channels (*such as school email address/ntlp address or school phone numbers*). Staff must not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/manager.
Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with schools policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
Members of staff are encouraged not to identify themselves as employees of Southridge First School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.

Member of staff will ensure that they do not represent their personal views as that of the school on social media.
School email addresses will not be used for setting up personal social media accounts.

3.3 Pupils use of social media

3.5

Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
Any official social media activity involving pupils will be moderated by the school where possible.
The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

4.1

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members Southridge First School community to take steps to ensure that mobile phones and personal devices are used responsibly.
The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including the school Acceptable Use Policy.
Southridge First School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

4.2

Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
Mobile phones and personal devices are not permitted to be used in certain areas within the school site/ activities such as changing rooms, toilets and swimming pools. They should not be used in classrooms during teaching time or when pupils are in the area. No phones should be on the yard with pupils or staff at lunch or playtime.
The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
North Tyneside / Kier staff are not to use phones in the school building except for the caretakers phone which will alert them of any issues and does not contain a camera. Members of staff will be issued with a school phone number and email address where contact with pupils or parents/carers is required.
Leasing contractors must comply with the e-safety policy as part of their conditions of lease or Transfer of Control agreement.
All members of Southridge First School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
All members of Southridge First School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
All members of Southridge First School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.

4.3 Pupils use of personal devices and mobile phones

4.3

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.

If parents request that pupils have access to a mobile phone e.g. in Year 4 some pupils walk home unaccompanied in the summer term then they will need to be handed in at the school office in the morning and collected at the end of the day.
If a pupil needs to contact his/her parents/carers the office staff will make contact on their behalf.
If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers at the end of the school day.

4.5 Staff use of personal devices and mobile phones

4.5

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-exiting relationships which could compromise this must be discussed with leaders/managers.
Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
If a member of staff breaches the school/setting policy then disciplinary action will be taken.
If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted and allegations will be responding to following the allegations management policy.

4.6 Visitors use of personal devices and mobile phones

4.6

Parents/carers and visitors must use mobile phones and personal devices in accordance with the schools policy.

We understand that many parents want to take photographs and videos of their own children at special school events such as Sports Day and Christmas Plays. Parents will be advised at the beginning of an event that they are unable to take whole school /group photographs or videos and that they may only take a photograph of their child at the end of the Christmas Performance. At Sports Events children may take a photograph of their own child at the end. We trust parents and carers to behave responsibly and ask that they ensure that any images they take will not be used inappropriately.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

5.1

Southridge First School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Schools should include appropriate details about the systems in place in line with North Tyneside provision services
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
The school will audit technology use to establish if the online safety (e-Safety) policy is adequate and that the implementation of the policy is appropriate.
Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.
Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the schools leadership team and governors.

5.2. Internet use throughout the wider school/setting community

5.2 The school will liaise with local organisations to establish a common approach to online safety (e-Safety).

The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

5.3 Authorising internet access

5.3

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
All staff, pupils and visitors will read and sign the School Acceptable Use Policy before using any school ICT resources.
Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

6.1

An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
Education about safe and responsible use will precede internet access.
Pupils input will be sought when writing and developing school online safety policies and practices.
Pupils will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
All users will be informed that network and Internet use will be monitored.

- Pupil instruction regarding responsible and safe use will precede Internet access.
- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study covering both safe school and home use.
- The pupil Acceptable Use expectations and Posters will be posted in classrooms, IT room and Community Room with Internet access. All users within these rooms must comply and sign agreement for use/
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

6.2 Engagement and education of children and young people who are considered to be vulnerable

6.2 Southridge First School are aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability

appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

6.3 Engagement and education of staff

6.3:

The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
To protect all staff and pupils, the school will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
The school, facilitated through ICT lead, will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

6.4

Southridge First School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, the school prospectus and on the school website.
A partnership approach to online safety at home and at school with parents will be encouraged.
Parents will be offered an annual e-safety session highlighting on line safety at home. Parents also will be requested to read online safety information as part of the Home School Agreement.
Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
Information and guidance for parents on online safety will be made available to parents via the school website.

7. Managing Information Systems

7.1 Managing personal data online

7.1

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
Full information regarding the schools approach to data protection and information governance can be found in the schools data protection policy.

7.2 Security and Management of Information Systems

7.2

The security of the school information systems and users will be reviewed regularly.
Virus protection will be updated regularly.
Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
Portable media may not be used without specific permission followed by an anti-virus /malware scan.
Unapproved software will not be allowed in work areas or attached to email.
Files held on the school's network may be regularly checked.
The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
All users will be expected to log off or lock their screens/devices if systems are unattended. Time enabled locking will be placed on all computer screens for staff. Devices must not be left accessible without a member of staff present.

Password policy

All users will be informed not to share passwords or information with others and not to login as another user at any time.
Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
All pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
We require staff and pupils to use STRONG passwords for access into our system.

7.3 Filtering Decisions

7.3

The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
The school uses North Tyneside educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils.
The school uses North Tyneside Council filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
The school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.
The school will work with North Tyneside Council and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
All changes to the school filtering policy will be logged and recorded.
The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate in collaboration with ICT technician and seek advice from North Tyneside Council.
Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

7.4

The headteacher/manager is ultimately responsible for the security of any data or images held of children. Ipads securing data or images should always be locked away and remain on the school site unless permission is granted from Headteacher or Deputy Head.
Apps/systems which store personal data will be risk assessed prior to use.
Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainment or photographs.

Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft. If this cannot be fully assured then they will not be taken off site.
Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

Responding to Online Incidents and Concerns

Relevant for all settings

8. All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
Complaints about Internet misuse will be dealt with under the School's complaints procedure.
Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure
Any complaint about staff misuse will be referred to the head teacher
Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
Pupils, parents and staff will be informed of the schools complaints procedure.
Staff will be informed of the complaints and whistleblowing procedure (Available on the Safeguarding Board in the staff room)
All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
The school will inform parents/carers of any incidents of concerns as and when required.
After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the LCSB or Northumbria Police via 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to North Tyneside Police.
If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Safeguarding Team to communicate to other schools/settings in North Tyneside.
Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions reading online safety concerns and has been written with input from specialist services and teams. This content is not exhaustive and cannot cover every eventually so professional judgement and support from appropriate agencies such as the LCSB Safeguarding Team, Police, CSET and Children's Social Care is encouraged.

Some settings may not feel that these sections are relevant due to the age and ability of children; however it is recommended that designated safeguarding leads ensure that their settings safeguarding policies and procedures are robust and are applicable for a range of safeguarding issues should they occur.

Some schools and settings will place these sections within existing safeguarding and child protection policies and procedures rather than the online safety policy or within other appropriate policies and procedures. Other settings will prefer to keep this content as reference material for Designated Safeguarding Leads.

9.1. Responding to concerns regarding Online Child Sexual Abuse

9.1.

Southridge First School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

Southridge First School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the North Tyneside Council LADO/Front Door and/or Police.
If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant North Tyneside procedures.
- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform North Tyneside police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.2. Responding to concerns regarding Indecent Images of Children (IIOC)

9.2

Southridge First School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or North Tyneside Police.

If the school/setting are made aware of Indecent Images of Children (IIOC) then the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant North Tyneside Safeguarding Child Boards procedures.
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.

If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

- Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.

Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
Follow the appropriate school policies regarding conduct.

9.3. Responding to concerns regarding radicalisation or extremism online

9.3.

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections.
When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

9.4.Responding to concerns regarding cyberbullying

9.4

Cyberbullying, along with all other forms of bullying, of any member of Southridge First School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
All incidents of online bullying reported will be recorded.
There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence and give a copy to the school.
The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.

- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.