Stanford Infant School

Online Safety Policy
2017

CONTENTS	PAGE
1. **Creating an Online Safety Ethos**	3
1.1 Aims and Policy Scope	3
1.2 Writing and Reviewing the Online Safety Policy	4
1.3 Key Responsibilities for the Community	4
1.3.1 Key Responsibilities for the SLT	4
1.3.2 Key Responsibilities of the DSL & OSL	5
1.3.3 Key Responsibilities for all Members of Staff	6
1.3.4 Staff Managing the Technical Environment	7
1.3.5 Children	8
1.3.6 Parents and Carers	8
2. **Online Communication and Safer Use of Technology**	9
2.1 Managing the School Website	9
2.2 Publishing Images and Videos Online	9
2.3 Managing Email	10
2.4 Official Videoconferencing and Webcam use for Educational Purposes	11
2.5 Appropriate and Safe Classroom use of the Internet and any Associated Devices	12
3. **Social Media Policy**	13
3.1 General Social Media Use	13
3.2 Official Use of Social Media	14
3.3 Staff Personal Use of Social Media	14
3.4 Pupils Use of Social Media	16
4. **Use of Personal Devices and Mobile Phones**	17
4.1 Rationale regarding Personal Devices and Mobile Phones	17
4.2 Expectations for Safe Use of Personal Devices and Mobile Phones	17
4.3 Staff Use of Personal Devices and Mobile Phones	18
4.4 Visitors Use of Personal Devices and Mobile Phones	19
5. **Policy Decisions**	19
5.1 Reducing Online Risks	19
5.2 Internet Use Throughout the Wider School Community	20
5.3 Authorising Internet Access	20
6. **Engagement Approaches**	20
6.1 Engagement and Education of Children	21
6.2 Engagement and Education of Children considered to be Vulnerable	22
6.3 Engagement and Education of Staff	22
6.4 Engagement and Education of Parents and Carers	22
7. **Managing Information Systems**	23
7.1 Managing Personal Data Online	23
7.2 Security and Management of Information Systems	23
7.3 Password Policy	24
7.4 Filtering and Monitoring	24
8. **Management of Applications (apps) Used to Record Children's Progress**	25
9. **Responding to Online Incidents and Safeguarding Concerns**	26
Appendix A – Procedures for Responding to Specific Online Incidents or Concerns	28
Appendix B – Questions to Support DSL's Responding to Concerns Relating to Youth Produced Sexual Imagery	34
Appendix C – Online Safety (e-safety) Contacts and References	36

1. Creating an Online Safety Ethos

A holistic approach has been taken to writing the Online Safety Policy to ensure that safe practice for all members of the school community is embedded.

At Stanford Infant School we celebrate <u>friendship</u>, <u>respect</u>, <u>excellence</u> and <u>courage</u>. Our safe and happy learning environment engages, challenges and *inspires* our learners on the beginning of a journey of learning forever.

'Exploring and Learning Together, Inspiring Each Other'

1.1 Aims and Policy Scope

Stanford Infant 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, tablets, mobile phones or games consoles.
- 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 and be empowered to build resilience online.
- has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Stanford Infant School's 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 Stanford Infant School is a safe and secure environment.
- Safeguard and protect all members of Stanford Infant School community online.
- Raise awareness with all members of the community regarding the potential risks as well as benefits of technology.
- 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, tablet 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, Use of Images, Acceptable Use Policies, Confidentiality and relevant curriculum policies including Computing, Personal Social and Health Education (PSHE); including Sex and Relationships Education (SRE).

1.2 Writing and Reviewing the Online Safety Policy

The Designated Safeguarding Lead (DSL) is: Emma Remnant

The Online Safety Lead is: Madeleine Denyer

The Online Safety Lead for the Governing Body is: Damian Fisher

The date for the next policy review is: February 2018.

The Online Safety Policy has been written by the school, involving staff, pupils and parents/carers.

The Online Safety (e–Safety) Policy and its implementation will be reviewed by the school at least annually or sooner if required. This is to reflect changes and advancements in technology or following any local or national guidance or legislation changes.

1.3 Key Responsibilities for the Community

All members of the school community have an essential role to play in ensuring the safety and well-being of others, both on and offline. It is important that all members of the community are aware of these roles and responsibilities and also how to access and seek support and guidance.

1.3.1 The Key Responsibilities of the School Leadership Team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.

- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety, including an Acceptable Use Policy, which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting 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.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school 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 ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

1.3.2 The Key Responsibilities of the Designated Safeguarding Lead and Online Safety Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.

- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need.
- To report to the School Leadership Team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the Local Authority and other local and national bodies, as appropriate.
- Working with the school Leadership Team to review and update the Online Safety Policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that Online Safety is integrated with other appropriate school policies and procedures.

1.3.3 The Key Responsibilities for all Members of Staff

All members of staff play an essential role in creating a safe culture within the school, both on and offline. All members of staff should seek to promote safe and responsible online conduct with and by children as part of the curriculum and as part of their safeguarding responsibilities. All members of staff will need to role model positive behaviours when using technologies, either directly with children or in the wider context. All staff should be aware of and ensure they adhere to the school Acceptable Use Policies (AUP's).

The key responsibilities of all members 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 systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- 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.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

1.3.4 Staff Managing the Technical Environment

Members of staff who are responsible for managing the school technical environment have an essential role to play in establishing and maintaining a safe online environment and culture. Staff with responsibility for the technical environment should work closely with the Leadership Team to provide expertise relating to appropriate education use of ICT systems and also to ensure that learning opportunities are not unnecessarily restricted to technical safety measures.

In addition to the above, the Key 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 Senior Leadership 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 DSL.
  Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
  Report any breaches or concerns to the DSL and Leadership Team and together ensure that they are recorded 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 DSL 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 staff.

1.3.5 Children

Children should be encouraged and empowered to develop safe and responsible online behaviours over time which will enable them to manage and respond to online risks as they occur.

The key responsibilities of children are:

- Contributing to the development of Online Safety Policies.
- Reading the school's 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 Parents and Carers

Parents/Carers play a crucial role in developing children's safe and responsible online behaviours, especially where a majority of children's access will be taking place when they are not in the school. Stanford Infant School is committed to working in partnership with families to raise awareness of online safety issues. Through this approach, parents/carers can help school to reinforce online safety messages and promote and encourage safe online behaviours wherever, and whenever, children use technology. Online Safety messages will be shared and promoted with parents/carers through a variety of communication channels and events throughout the year. The Online Safety Page on the School's Website will be regularly updated to reflect this.

The key responsibilities of parents and carers are:

- Reading the school's 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 technology and social media.
- 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's online safety policies.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

The school uses a variety of online communication and collaboration tools both informally and formally with the school community. The school needs to provide clear boundaries and expectations for safe use.

2.1 Managing the School Website

Schools are required to publish certain information online. The most recent guidance on what school's must publish online can be found here: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- 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 and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Pupils work will 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.
- The school will post information about safeguarding, including online safety, on the School Website for members of the community.

2.2 Publishing Images and Videos Online

Still and moving image and sound add liveliness and interest to a publication or website. Nevertheless, the security of staff and pupils is paramount. Images of a child will not be published with the parent's/carer's permission.

- The school will ensure that all images and videos shared online are used in accordance with the school Use of Image Policy.
- The school will ensure that all use of images and videos take place in accordance other policies and procedures including Data Security, Acceptable Use Policies and Codes of Conduct.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing Email

Email is an essential method of communication for staff and parents/carers.

- Pupils may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school 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 (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Whole -class or group email addresses may be used for communication outside of the school.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents/carers.
- Email sent to external organisations should be written carefully and, if appropriate, authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official Videoconferencing and Webcam use for Educational Purposes

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. Videoconferencing introduces exciting dimensions for educational contexts.

- The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content
- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.

- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, the school will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and Safe Classroom use of the Internet and any Associated Devices

Developing safe and effective practice in using the internet for teaching and learning is essential. All members of staff muse be aware that no search engine or filtering tool is ever completely safe, and appropriate supervision, use of safe search tools (where possible), pre-checks of search terms, age appropriate education for pupils and robust classroom management must always be in place.

- 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. Please access specific curriculum policies for further information.
- 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.
- 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
    - 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.
    - 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.
    - All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- 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 ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- 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.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3. Social Media Policy

Schools should acknowledge that there are significant potential benefits for communication, engagement, collaboration and learning via the internet and social media.

3.1 General Social Media Use

- Expectations regarding safe and responsible use of social media will apply to all members of the school community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the 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 the school community.
- All members of the 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 use of social networking applications during school hours for personal use is not permitted.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the leadership team and will be managed in accordance with 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 relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official Use of Social Media

- The only official social media channels are the PTFA Facebook Closed Group.
- Official use of social media sites by the school will only take place with clear community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Head Teacher.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including Anti-Bullying and Child Protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the Use of Images Policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and l action taken to safeguard the community.
- Public communications on behalf of the school will, where possible, be read and agreed by two formal administrators of the site.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff Personal Use of Social Media

All members of staff will be made aware of the potential risks of using social networking sites or personal publishing both professionally and personally. Members of staff should understand the importance of considering the material they post online and the need to ensure that their personal profiles are secured or set to private.

- The safe and responsible 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 children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Head Teacher.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head Teacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
- Information and content that 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 to ensure that their social media use is compatible with their professional role and is in accordance with school's policies (Safeguarding, 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 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.
- Members of staff are encouraged not to identify themselves as employees of Stanford Infant 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 community.
- Members 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.

3.4 Pupils Use of Social Media

Social Media is now an everyday form of communication for many children and forms a vital part of growing up in today's modern Britain and wider global society. Social Media sites are blocked at school' however, it cannot be assumed that they will not access them off-site when using personal devices. It is therefore essential that children are given age appropriate education regarding safe and responsible use and are also appropriately exposed to social media sites to enable them to develop and build skills and resilience.

- Safe and responsible use of social media sites will be outlined for children and their parents/carers as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- 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 concerns regarding pupils' use of social networking, social media and personal publishing sites, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

Due to the widespread use of a range of internet enabled personal devices, it is essential that schools take steps to ensure all mobile phones and personal devices are used responsibly.

4.1 Rationale regarding Personal Devices and Mobile Phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The school recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools.

4.2 Expectations for Safe Use of Personal Devices and Mobile Phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Electronic devices of all kinds that are brought in on site 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, i.e. where children are present.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- All members of the school community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the 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 the 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.
- School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Staff Use of Personal Devices and Mobile Phones

The use of mobile phones by staff for making/taking calls or sending/receiving texts, etc., is not allowed when children are present and they must not be used in the communal areas of the school. During contact tile they should be switched off or on silent and put away. They are allowed when children are not present or in the designated staff areas; the Staffroom and the Staff Workroom. Staff should not use a mobile phone during contact time, unless in specific circumstances at the discretion of the Head Teacher.

- Members of staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with their Line Manager.
- 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.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. Confidentiality, Data Security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during school hours.
- Bluetooth or other forms of communication should be 'hidden' or switched off during lesson times.
- 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 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.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management policy.

4.4 Visitors Use of Personal Devices and Mobile Phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's Acceptable Use Policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school Use of Image Policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- 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

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed.

5.1 Reducing Online Risks

- Stanford Infant 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 and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- 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 always possible to guarantee that

access to unsuitable material will never occur via a school/setting 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 School's Leadership Team.

5.2 Internet Use Throughout the Wider School Community

Internet access is available in many situations in the Local Community.

- The school will liaise with local organisations to establish a common approach to online safety.
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- 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

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents/Carers will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents/Carers will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the 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

Online Safety forms an important part of the Computing Curriculum Programmes of Study for children within schools and this highlights the importance for children to use technology safely and respectfully, understand how to keep personal information private and be able to identify where to go for help and support when they have concerns about content or

contact on the internet or other online technologies from an increasingly early age. Children will need to develop an understanding on how to become safe and responsible online or digital citizens and this is developed within an appropriate Personal, Social and Health Education (PSHE) curriculum.

Whilst the Computing Curriculum forms an essential part of online safety education for children, safe and responsible use of technologies is embedded throughout the whole school curriculum to ensure children develop the required range of digital literacy and safety skills as well as to develop online resilience to enable them to become safe and responsible internet users.

- 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, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the 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.
- Online Safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing Programmes of Study, covering both safe school and home use.
- Online Safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety (e-Safety) education approaches.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

6.1 Engagement and Education of Children considered to be Vulnerable

Children may be considered vulnerable for a variety of reasons. This could include: children with special educational needs, children with mental health need, children in care, children who have experienced trauma and abuse, children with low self-esteem, children with English as an Additional Language, etc. Whole school strategies are established in order to protect a wide cohort of

children to enable us to support the individual needs that vulnerable pupils may display.

- Stanford Infant School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- Stanford Infant School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked After Child Leader).

6.2 Engagement and Education of Staff

Online Safety Training is revisited annually as part of Safeguarding Training for all staff to ensure that the online safety culture is clearly established and implemented and to ensure that all staff understand how to protect both children and themselves as professionals.

- The online 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 our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- 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 in a variety of ways, on a regular (at least annual) basis.
- 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.
- 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 will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.3 Engagement and Education of Parents and Carers

Parents and carers form a vital element in the approach to teaching and empowering children to become safe and responsible digital citizens. By working together, parents and carers, schools and other professionals can help to reinforce online safety messages and can encourage positive behaviour wherever and whenever children go online.

- Stanford Infant School recognises 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'/Carers' attention will be drawn to the school online safety policy and expectations in Newsletters, Letters and on the School Website.
- A partnership approach to online safety at home and at school with parents/carers will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings.
- Parents/Carers will be requested to read online safety information as part of the Home School Agreement.
- Parents/Carers 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/carers in a variety of formats.
- Parents/carers will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing Personal Data Online

- 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 School's Information Security Policy.

7.2 Security and Management of Information Systems

- 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 will be regularly checked.

- The Computing Leader/Network Manager will review system capacity regularly.
- 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.
- The school will log and record internet use on all school owned devices.

7.3 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.
- We require staff and pupils to use STRONG passwords for access into our system.

7.4 Filtering and Monitoring

- The Governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- 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.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity through BHCC which is appropriate to the age and requirement of our pupils.
- The school uses filtering via Smoothwall which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will work with BHCC and the 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.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Brighton and Hove Police or CEOP immediately.

8. Management of Applications (apps) Used to Record Children's Progress

A number of applications (apps) for mobile devices have been launched which are targeted specifically at education settings which allow staff to track and share a child's learning journey online with parents and carers. Such tools have considerable benefits for schools and their communities, including improved engagement with parents/carers and reduction in paperwork. Careful consideration is given to safeguarding and data security principles before using such tools.

- The Head Teacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents/Carers will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

9. Responding to Online Incidents and Safeguarding Concerns

Internet technologies and electronic communications provide children with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, 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 DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the BHCC Safeguarding Children's Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's Complaints Procedure.
- Complaints about online/cyber 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 school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- 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 Education Safeguards Team or Brighton and Hove Police via 101 or 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 Brighton and Hove 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 community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Brighton and Hove.
- Parents/Carers and children will need to work in partnership with the school to resolve issues.

<u>Appendix A</u>

Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or 'Sexting'

- Stanford Infant School ensures that at all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as 'sexting').
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The school views 'sexting' as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead, Emma Remnant.
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- If the school are made aware of incident involving creating youth produced sexual imagery the school will:
    - Act in accordance with the school's Child Protection and Safeguarding Policy and the relevant Brighton and Hove Safeguarding Child Boards procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the children(s) involved.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

- Inform parents/carers about the incident and how it is being managed.
- The school will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school's network or devices, then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- Stanford Infant 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.
- Stanford Infant 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 Education Safeguarding Team and/or the Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DSL.
- 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 school's Child Protection and Safeguarding Policy and the relevant Safeguarding Children's Boards procedures.
    - Immediately notify the Designated Safeguarding Lead.

- Store any devices involved securely.
- Immediately inform the police via 101 (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
- 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.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- 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.

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

- Stanford Infant 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 the Police.
- If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the school's Child Protection and Safeguarding Policy and the relevant Safeguarding Children's 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), the 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 school's 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.

9.4. Responding to Concerns regarding Radicalisation and Extremism Online

- 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.
- 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 Child Protection and Safeguarding Policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or the Police.

Responding to Concerns regarding Cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of Stanford Infant 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 the Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- 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.

Responding to Concerns Regarding Online Hate

- Online hate at Stanford Infant School will not be tolerated. Further details are set out in the school policies regarding Anti-Bullying and Behaviour.
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with the school's Anti-Bullying Policy.
- The Police will be contacted if a criminal offence is suspected. 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 the Police.

Written by: Madeleine Denyer
Agreed by Staff: 3rd April 2017
Ratified by Governors: 4th April 2017

This policy is based on the work of the KSCB Online Safety (-safety) strategy group.

Appendix B

Questions to support DSL's responding to concerns relating to Youth Produced Sexual Imagery

The following statements may support DLS's in considering how best to respond to concerns relating to youth produced sexual imagery:

Child Involved:

- What is the age of the child(ren) involved?
    - If under 13 then a consultation/referral to Children's Social Care should be considered.
    - If an adult (over 18) is involved, then Police involvement will be required. Contact 101 or 999 if there is risk of immediate harm.
- If the child is able to understand the implications of taking/sharing sexual imagery?
- Is the school or other agencies aware of any vulnerability for the children involved? E.g. special educational needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and well-being of the child(ren) involved? E.g. family situation, children are risk of sexual exploitation.

Context

- Is there any contextual information to help inform decision making?
    - Is there indication of coercion, threats, blackmail?
    - What was the intent for taking/sharing the imagery? E.g. was it a 'joke' or are the children involved in a 'relationship'?
    - If so, is the relationship age appropriate? For Primary Schools, a referral to social care regarding under age sexual activity is likely to be required.
        - Is this behaviour age appropriate experimentation, natural curiosity or is it possible exploitation?
- How were the school made aware of the concern?
    - Did a child disclose about receiving, sending or sharing imagery themselves or was the concern raised by another pupil or member of the school community? If so, how will the school safeguard the pupil concerned given that it is likely to be distressing to discuss.
- Are there other children/pupils involved?
    - If so, who are they and are there any safeguarding concerns for them?
    - What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)?

- Is the imagery on a school device or personal device? Is the device secured?
  - **NB: Schools must NOT print/copy, etc., imagery suspected to be indecent – the device should be secured until advice can be obtained.**

The Imagery
- What does the school know about the imagery? (be aware it is unlikely to be necessary for staff to view the imagery)
  - Is the imagery potentially indecent (illegal) or is it 'inappropriate'?
  - Does it contain nudity or sexual acts?
- Does the child(ren) know who has accessed the imagery?
  - Was it sent to a known peer (e.g. a friend) or a known or unknown adult?
- How widely has the imagery been shared? E.g. just to one other child privately, shared online publically or sent to an unknown number of children/adults?

Action
- Does the child need immediate support and/or protection?
  - What is the specific impact on the child?
  - What can the school put in place to support them?
- Is the imagery available online?
  - If so, have appropriate reports been made to service providers, etc.?
- Are other schools/settings involved?
  - Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in youth produced sexual imagery concerns before?
  - If so, what action was taken? NB: repeated issues will increase concerns for offending behaviour and vulnerability, therefore an appropriate referral will be required.
- Are the school Child Protection and Safeguarding Policies and Practices being followed?
  - Is a member of the Child Protection Team on hand and is their advice and support available?

* How will the school inform parents/carers?

With older pupils it is likely that DSL's will work with the young person to support them and to inform parent/carers.

Can the school manage this issue internally or are other agencies required?

Issues concerning adults, coercion or blackmail, violent/extreme imagery, repeated concerns, vulnerable pupils or risk of significant harm will always need involvement with other agencies.

DSL's should follow guidance available locally by the BHCC and Education Safeguarding Team and nationally via 'Sexting in schools: youth produced sexual imagery and how to handle it'.

Appendix C
Online Safety (e-Safety) Contacts and References

Brighton and Hove Support and Guidance

Brighton and Hove Education Safeguarding Team:
Safethttp://www.brightonandhovelscb.org.uk/parents/par_esafety/y Support for Education Settings.

Brighton and Hove Police:
In an emergency (a life is in danger or crime in progress) dial 999. For other non-urgent enquires contact Brighton and Hove Police via 101.

BHCC Local Safeguarding Children Board (LSCB)
http://www.brightonandhovelscb.org.uk/

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre):
www.ceop.police.uk

ChildLine: www.childline.org.uk

 Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline:
www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/