St Nicholas CE Primary

Online Safety Policy

'Joyful is the person who finds wisdom' Proverbs 3:13-15

Part of the Safeguarding Strategy

See also policies on Child Protection, Behaviour Policy, Anti-Bullying, Internet Policy, Acceptable Use, Mobile Devices, Data Protection /Security Policy and Complaints

Approved by:	St Nicholas CE Primary School Governing Body	**Date:**	
Last reviewed on:			
Next review due by:	September 2021		

1. Aims and objectives

New technologies have become integral to all our lives in today's society – and not least to children. Children will need to develop high-level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

The internet and associated technologies are powerful tools for learning. They have the potential to access information at high speed and to empower children to take an increased level of ownership over their learning. The use of the internet and associated technologies in school are tools that provide our children with exciting opportunities to pursue 'personalised learning'.

The purpose of this policy is to ensure Online Safety risks are minimised, not only for children but for their parents and the other members of the school community through 3 key areas: Policies and practice; Education and training; and Infrastructure & technology. This will allow all members of the school community to make the most of the internet's potential (and its associated technologies) for learning and everyday living.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Build both an infrastructure and culture of Online Safety
- Ensure safe access to on-line material for all users
- Have an Acceptable Use Policy (AUP) for all members of the School Community, covering the conditions of responsible internet and technology use for all users including use of learning platforms such as our Virtual Learning Environment (VLE) through e-schools (both at home and school).
- Create guidelines that will lead to a safer online for children and will include filtering appropriate to the age of the children.
- Provide guidelines for internet use that is planned, task-orientated and educational within a regulated and managed environment – that accords with our school's ethos. (This includes use by adults and children.)
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Ensure that children will be taught what is acceptable and what is not acceptable and given clear objectives for responsible Internet use - including: an ability to evaluate the quality, accuracy and relevance of information on the internet; plagiarism and copyright infringement; illegal downloading of music or video files.
- Ensure that children and teachers are aware of 'cyber-bullying', how to prevent it happening how to stop it if it occurs, and including how to report incidences.
- Provide information to parents to enable them to both support and proactively contribute to the school's Online Safety framework (including the potential for excessive use which may impact on the social and emotional development and learning of their children)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good

reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is the governor for safeguarding.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet. Acceptable Use Policy (AUP) (Appendix 3)

3.2 It is the responsibility of the Headteacher to:

- Ensure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 It is the responsibility of the Senior Leadership Team (SLT) to:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure 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. Audit and evaluate online safety practice to identify strengths and areas for improvement.

3.4 It is the responsibility of the designated safeguarding lead to:

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (Appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety.

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board

This list is not intended to be exhaustive.

3.5 It is the responsibility of staff managing the technical environment to:

Our technical environment is managed by Apollo Technology.

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Ensure that the schools filtering policy is applied and updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material; responsibility for its implementation is shared with the leadership team.
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

This list is not intended to be exhaustive.

3.6 It is the responsibility of all members of staff and volunteers to:

- Maintain an understanding of this policy
- Implement this policy consistently
- Read and adhere to the this policy and AUPs (Appendix 3)
- Work with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.

- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

This list is not intended to be exhaustive.

3.7 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs. (Appendices 1 and 2)
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

3.8 It is the responsibility of the parents and carers to:

- Read the school AUPs (Appendices 1 and 2) and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.9 It is the responsibility of visitors and members of the community to:

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Education and Engagement Approaches

4.1 Education and engagement with pupils

The Internet is an essential part of our lives today in education, business and social interaction. St Nicholas CE Primary has a duty to provide students with quality Internet access as part of their learning experience.

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Ensuring all pupils agree and sign an age appropriate agreement for using the internet responsibly [*also to be agreed in class rules*] at the beginning of each school year, which will be shared with parents and carers
- Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to respect copyright when using material found online and to acknowledge the source of information
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Teaching children the importance of not sharing personal information and photographs over the internet. As children get older it is particularly important that children are made aware of what is safe to share and how as older children cannot do certain things online without sharing some personal information.
- Being vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.

The school will support pupils to read and understand the AUP in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology by pupils.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.
- Using assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
- Pupils will be taught about online safety as part of the curriculum.

  In **Key Stage 1**, pupils will be taught to:

  - Use technology safely and respectfully, keeping personal information private
  - Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

  In **Key Stage 2** will be taught to:

  - Use technology safely, respectfully and responsibly
  - Recognise acceptable and unacceptable behaviour
  - Identify a range of ways to report concerns about content and contact
- The safe use of social media and the internet will also be covered in other subjects where relevant.

4.2 Education and engagement with vulnerable pupils

- At St Nicholas we are aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils and seek input from specialist staff as appropriate, including the SENCO and Social Care.

4.3 Educating parents about online safety

- St Nicholas CE Primary recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
- Raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE).
- Provide information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Draw their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Request that they read online safety information as part of joining our school, for example, within our home school agreement.
- Requiring them to read the school AUP and discuss its implications with their children.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

5. Acceptable use of the internet in school

- St Nicholas CE Primary recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP (Appendices 1 and 2) and highlighted through a variety of education and training approaches.
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- School computer systems (including audits of the safety and security of the systems) will be regularly reviewed with the ICT Technician
- Virus protection will be updated regularly

- Security strategies will be discussed with the Local Authority and the ICT Technician. See Guide for Appropriate Filtering and Monitoring (Sept 2016)

6. Reducing Online Risks

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Committee (or other group)

- Older children (generally accepted by Ofsted as KS2) should have individual passwords.

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

- The school ICT systems will be reviewed regularly with regard to security.

- The school will use SOPHOS Anti-Virus Protection. Updates will be administered by the school ICT technician.

- Files held on the school's network will be regularly checked by the Computing Leader and by class teachers. Where inappropriate material, or an excess of material, is found to be stored in an individual user file the necessary action will be taken to rectify the problem. This might lead to school disciplinary action

6.1 Classroom Use

- St Nicholas CE Primary uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - School learning platform/intranet
    - Email
    - Games consoles and other games based technologies
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools, 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 always be supervised when using the internet.

6.2 Managing Internet Access

- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

6.3 Filtering and Monitoring

6.3.1 Decision Making

- Governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

6.3.2 Filtering

- The school uses educational broadband connectivity through South West Grid for Learning (SWGfL). This system provides three tiers of filtering safety.
- RM SafetyNet provides a filter service for all schools as part of the SWGfL. This is updated constantly using information from Local Education Authorities, web-based watch dogs and from research carried out by RM themselves.
- This service is refined by the Local Authority (LA), who receives information from schools regarding inappropriate sites that have slipped through the filter.
- The school uses RM Safety Net which blocks sites which can be categorised as: violence, pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school works with RM SafetyNet who provide a filter service for all schools as part of the SWGfL to ensure that our filtering policy is continually reviewed.
- Schools have a local facility to block specific sites or keywords from searches. This ensures maximum and immediate high level filter protection.
- This provision is in addition to standard filtering software installed on each PC as standard which will also be set at maximum.
- Children do not have unauthorised access to the internet. Younger children will be supervised by a member of staff when accessing on-line material.
- Children will be guided to suitable web sites – pre-checked as suitable for their use. Often blocks are put in place by the school on sites deemed not suitable
- Rules for responsible Internet access will be posted near all computer systems and children helped to understand them (Appendix 4)
- All users will be taught how to use learning platforms safely and responsibly and all members will have their own user name and password.
- Children will be informed that Internet use will be monitored.

6.3.3 Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.

- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Police or CEOP.

6.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices.
- Any breaches in use will be reported to the Headteacher.
- 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.

6.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998 and in compliance with the General Data Protection Regulation (GDPR) May 2018.
- Full information can be found in the schools GDPR Policy.
- The South West Grid for Learning (SWGfL) Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.
- The school will:
    - at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
    - use personal data only on secure password protected computers and other devices
    - ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data
    - store or transfer data using encryption and secure password protected devices *(data via email without password encryption is not always deemed as secure)*
    - ensure laptops and USBs are encrypted if personal data for pupils is being taken off-site
    - make sure data is deleted from the device once it has been transferred or its use is complete

6.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems. This is currently being implemented.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on the school's network,
    - The appropriate use of user logins and passwords to access the school network.
    - Specific user logins and passwords will be enforced for all but the youngest users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found in the GDPR Policy.

6.5.1 Password policy

- 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.

- From year 3 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 all users to:
    - Use strong passwords for access into our system.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

6.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.
- Class teachers will have overall responsibility for the content published on their class pages.

6.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): GDPR Policy, AUPs, Codes of conduct and Social media.
- A general written permission note from parents/carers will be obtained so that the school can use images in newsletters and online.
- Staff will only take images on the school devices.
- Photographs and video taken within school are used to support learning experiences across the curriculum, as well as to provide information about the school on the website
- When using digital images, pupils should be educated about the risks associated with the taking, use, sharing, publication and distribution of images (including on social networking sites)
- Images or videos that include pupils will be selected carefully and will not provide material that could be reused
- Photographs or video are not to be taken in school for any purpose by members of the public without permission from the Headteacher/Senior Management Team.
- Schools could encourage parents/carers to consider the following ideas before they share photos or videos online [from the Information Commissioners Office]:
    - Some children and adults are at risk and MUST NOT have their image put online. Not all members of the school community will know who they are – so ALWAYS ask permission before sharing photos or videos online
    - Once posted and shared online any image or video can be copied and will stay online forever
    - Some people do not want their images online for personal or religious reasons
    - Some children, families and staff may have a complex family background which means that sharing their image online can have unforeseen consequences

- In order to keep all members of the school community safe we must all 'Think Before We Post' photos and videos online

6.8 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.
    - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Headteacher if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

6.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
- All members of staff are provided with a specific school email address, to use for all official communication.
- Any communication over email between staff and parents will be via the school email system i.e. using a bathnes.gov.uk email address (or via School office)
- All communication between adults and children through the school messaging system on the VLE will take place within clear and explicit professional boundaries.
- Adults will not share any personal information with a child and they should not request or respond to any personal information form the child other than that which might be appropriate as part of their professional role.
- Adults MUST ensure that all communications are transparent and open to scrutiny.
- Any offensive emails must be reported to the Headteacher/SMT
- Staff should not contact pupils via personal email
- Staff must use children's initials in emails and use encrypted memory sticks when transferring data
- Any user found to be using e-mail for sending inappropriate messages will be subject to school discipline procedures.
- Members of staff are encouraged to have an appropriate work life balance when responding to email.

6.8.2 Pupils

- Pupils may use a school provided email accounts for educational purposes.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the school.

6.9 Management of Learning Platforms

- St Nicholas CE Primary uses e-schools as its Virtual Learning Environment (VLE)
- Leaders and staff will regularly monitor the usage of the VLE in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the VLE
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.

- Pupils and staff will be advised about acceptable conduct and use when using the VLE.
- All users will be mindful of copyright and will only upload appropriate content onto the VLE.
- Any concerns about content on the VLE will be recorded and dealt with in the following ways:
    - The material will be removed by the site administrator.
    - Access to the VLE for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement. A pupil's parent/carer may be informed.
    - If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.
- 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.

6.10 Management of Applications (apps) used to Record Children's Progress

- The school uses Tapestry in the EYFS to track pupils' progress and share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation
- In order to safeguard pupils data:
    - 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.
    - School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.
    - Parents will sign a consent form allowing images of their children to be uploaded onto Tapestry.

7. Social Media

7.1 Expectations

- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the school's code of conduct. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.
- The guidance contained in this policy is an attempt to identify what behaviours are expected of adults within the school setting who work with or have contact with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may

bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

- Adults within the school setting should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.
- All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times.
- 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 school will control pupil and staff access to social media whilst using school provided devices and systems on site.
- The use of social media during school hours for personal use by staff is permitted during their breaks.
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of school community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Safeguarding policies.

7.2 Staff personal Use of Social Media

- 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 Code of conduct within the AUP.

7.3 Protection of personal information

- Managing personal information effectively makes it far less likely that information will be misused.
- In their own interests, adults within school settings need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.
- Adults working in schools should:
    - Never share their work log-ins or passwords with other people.
    - Keep their personal phone numbers private
    - Not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address should be used.
    - Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.
    - Only equipment and Internet services provided by the school or setting.
    - Follow their school/setting's Acceptable Use policy.
    - Ensure that their use of technologies could not bring their employer into disrepute.
    - Ensure that confidentiality is considered at all times. Social media has the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.
    - Ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social media (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Bath and North East Somerset Council could result in formal action being taken against them.

- Remember that they must comply with the requirements of equalities legislation in their on-line communications.

- Adults working in schools should *not*:
  - Use school ICT equipment for personal use, e.g. camera or computers.
  - Use their own mobile phones to contact pupils or parents except in exceptional circumstances when they should withhold their number.
  - Post derogatory remarks or offensive comments on-line or engage in online activities which may bring the school or Bath or North East Somerset Council into disrepute or could reflect negatively on their professionalism.
  - Put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the Local Authority.

- All adults, particularly those new to the school setting, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may undermine their professional position if they are published outside of the site.
- Staff should not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work.

7.4 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may 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.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites as strictly as they can.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of St Nicholas CE Primary 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.
- 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 schools policies and the wider professional and legal framework.
- 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 or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

7.5 Communication between pupils / adults working in school

- All members of staff are advised not to communicate with or add as ‘friends’ any current or past 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 headteacher.
    - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- 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 Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.
- The school provides a work mobile and e-mail address for communication between staff and pupils where this is necessary for particular trips/assignments. Adults should not give their personal mobile numbers or personal e-mail addresses to pupils or parents for these purposes.
- Adults should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.
- Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.
- Adults should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.
- E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school's policy.
- Adults should not establish or seek to establish social contact via social media / other communication technologies with pupils.

7.6 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- 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 specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised, through the e-safety curriculum to:
    - consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
    - only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - use safe passwords.
    - use social media sites which are appropriate for their age and abilities.
    - block and report unwanted communications and report concerns both within school and externally.

7.7 Official Use of Social Media

- St Nicholas CE Primary School's official social media channels are: **Facebook and Twitter**

- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
- Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Staff use school provided email addresses to register for and manage any official school social media channels.
- Official social media sites are suitably protected and, where possible, are linked to the school website.
- Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, GDPR, Confidentiality and Child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- 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.

7.8 Staff expectations when using School Social Media

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Sign the school's Social media acceptable use policy.
    - Be professional at all times and aware that they are an ambassador for the school.
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

7.9 Access to inappropriate images and internet usage

- There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the disciplinary action being taken.

- Adults should not use equipment belonging to their school/service to access any adult pornography; neither should personal equipment containing downloaded images be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.
- Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools need to ensure that internet equipment used by pupils has the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.
- Where indecent images of children are found, the police and local authority designated officer (LADO) should be immediately informed. Schools should refer to the dealing with allegations of abuse against adults policy and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.
- Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either HR or the LADO should be informed and advice sought. Schools should refer to the dealing with allegations of abuse against adults policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

7.10 Online bullying

- Online bullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'
- Prevention activities are key to ensuring that adults are protected from the potential threat of online bullying. All adults are reminded of the need to protect themselves from the potential threat of online bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.
- If online bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.
- Adults may wish to seek the support of their union or professional association representatives or another colleague to support them through the process. Employees will also have access to the Health Assured Employee Assistance Programme, telephone 0800 030 5182, a free 24 hour confidential counselling and advisory service, (subject to appropriate funding arrangements)
- Adults are encouraged to report all incidents of online bullying to their line manager or the headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

7.11 Parental use of social media

- Parents and carers will be made aware of their responsibilities regarding their use of social networking.
- Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.
- Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

7.12 Dealing with incidents of online bullying/inappropriate use of social networking sites

- The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.
- In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.
- The Governing Body understands that there are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged. Furthermore, laws of defamation and privacy still apply to the web and it is unlawful for statements to be written which:
    - expose (an individual) to hatred, ridicule or contempt
    - cause (an individual) to be shunned or avoided
    - lower (an individual's) standing in the estimation of right-thinking members of society or
    - disparage (an individual in their) business, trade, office or profession." (National Association of Headteachers)

8. Use of Personal Devices and Mobile Phones

- St Nicholas CE Primary recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

8.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour, Child protection and GDPR.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
- All members of the school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of the school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of the school community are 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 GDPR, Behaviour or Child protection policies.

8.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, GDPR and Acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.

- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless written permission has been given by the headteacher, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Headteacher.
    - If in an emergency situation staff should use 141 to protect the privacy of their number.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy
- 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, the police will be contacted.

8.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Pupils at St Nicholas CE Primary are asked not to bring mobile phones or devices into school. However, if parents request this for a specific purpose then the phone or device must be handed into the office to be kept secure until the end of the day.
- If a pupil needs to contact his/her parents or carers they will be allowed to use the office phone.

8.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection.
- The school will ensure appropriate signage and information is given to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

8.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

- School mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies.

9. Staff using work devices outside school

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the headteacher.
- Work devices must be used solely for work activities.

10. Responding to Online Safety Incidents and Concerns

- Staff will ensure that technology is being used appropriately to support learning and where possible will consider whether the technology has access to inappropriate 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.
- The School cannot accept liability for the material accessed, or any consequences resulting from internet use.
- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the BANES Safeguarding Children Board thresholds and procedures.

- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.
- Any user found to be in violation of the guidelines outlined in this policy will be subject to school discipline procedures. Repeated violations would cause that user to be banned from using the internet in school and in the case of adults, banned from working with children (amend as appropriate).

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

- The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the DSL.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

11.2 Online Child Sexual Abuse and Exploitation

- The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community. This can be accessed via the school website.

11.3 Indecent Images of Children (IIOC)

- The school will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
    - Act in accordance with the schools child protection and safeguarding policy
    - Immediately notify the school DSL.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, 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.
    - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, 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.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
    - Ensure that the headteacher is informed.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

11.4.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

11.4.2 Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- All incidents of cyberbullying reported to the school will be documented, recorded and investigated. Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- Staff will adhere to the following guidelines for helping the online bullying victim. (Please also refer to anti – bullying policy and the recent national guidance www.childnet.com/cyberbullying-guidance)
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

11.4.3 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at St Nicholas CE Primary and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or the Police.

11.4.4 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy and Prevent training.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Prevent training.

12. Training and engagement

12.1 Staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Ensure staff Initially sign and review of the Staff Acceptable Use Policy during Induction Safeguarding Interview
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates as part of staff training or as required.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.

- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

12.2 Pupils:

- Pupils will be taught Online Safety through PSHE and in other subjects where appropriate including the ICT curriculum and staff will reinforce Online Safety messages in the use of ICT across the curriculum to increase pupils' awareness of issues and how to deal with them.
- Online Safety guidelines will be clearly displayed by computers and children and young people will be made aware of these
- Pupils will understand that internet use will be regularly monitored and reviewed
- Children will be expected to sign the AUP.
- Children will be made very aware that a member of staff can see all changes and messages on the VLE and that improper use could result in the withdrawal of membership

12.3 Parents:

- Parents will be invited to attend any meetings held on Online Safety held in School or with other cluster schools.
- The online safety page of the website provides parents with a link to this policy and links to recommended websites which provide parents with information to support all children (and the wider school community) in staying safe as they use the internet and associated technologies.
- Parents will be asked to discuss and sign Acceptable Use Policy (AUP) on entry into school and then again in Year 3. (KS2)
- As part of the Online Safety curriculum, children will also receive any relevant information available to share with their family.
- Where specific advice is received from time to time through external sources such as 'Thinkuknow', it will be passed on to parents through school induction events/newsletters / emails/ website.

12.4 Governors:

- Governors will be given the opportunity to take part in Online Safety training / awareness sessions – particular the Governors with responsibility for ICT and Child Protection – through:
    - Attendance at training provided by the Local Authority / National Governors Association.
    - Participation in school training / information sessions for staff or parents
    - Regular reviews of the Internet Safety Policy
    - Signing their Acceptable Use Agreement

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Curriculum policies
- Social Media Policies

14. Monitoring arrangements

- This policy will be reviewed yearly or as appropriate by the Computing subject leader. At every review, the policy will be shared with the governing board.
- The DSL (Designated Safeguarding Lead) logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

Appendix 1: KS1 Acceptable Use Agreement (pupil and parents/carers)

St Nicholas CE Primary School

Use of the school's ICT systems and internet:
KS1 Acceptable Use Agreement for pupils and parents/carers

Name of pupil:

This is how we stay safe when we use computers:

- I will ask a teacher if I want to use the computers / tablets
- I will only use activities that a teacher has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I know the teachers can see what websites I visit

Parent/carer agreement:

- I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.
- I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.
- I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Social Media:

- I will not post any photos of pupils, other than my own children, on social networking sites where these photos have been taken at a school event.
- I will not post malicious or fictitious comments about the school or any members of the school community on social networking sites.
- I will make complaints through official school channels rather than posting them on social networking sites.

Signed (parent/carer):	**Date:**

Appendix 2: KS2 Acceptable Use Agreement (pupil and parents/carers)

St Nicholas CE Primary School

Use of the school's ICT systems and internet:
KS2 Acceptable Use Agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school:

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal use unless I have permission.
- I will only use technology with a teacher being present and with the teacher's permission
- I will not access any inappropriate websites, including social networking sites and chat rooms.
- I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not disclose or share personal information about myself or others (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will never arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that the school will monitor my use of the systems, devices and digital communications.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community. (e.g. cyberbulling)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to sanctions. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Signed (pupil):	**Date:**

Parent/carer agreement:

- I agree that my child can use the school's ICT systems and internet when appropriately

supervised by a member of school staff.

- I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.
- I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Social Media:

- I will not post any photos of pupils, other than my own children, on social networking sites where these photos have been taken at a school event.
- I will not post malicious or fictitious comments about the school or any members of the school community on social networking sites.
- I will make complaints through official school channels rather than posting them on social networking sites.

Signed (parent/carer):	**Date:**

Appendix 3: Acceptable Use Agreement (staff, governors, volunteers and visitors)

St Nicholas CE Primary School

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will thoroughly check any material which I intend to share with the children and understand that failure to do so may lead to disciplinary action.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I will adhere to the school's social media policy.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Computer Use Posters

St Nicholas CE Primary School
Computer Use Rules

1

ALWAYS ask an adult before using a computer.

2

ALWAYS use your own login and **NEVER** access other people's files. **ONLY** use the shared area when told to by a teacher.

3

ALWAYS be polite and sensible when communicating with others and when completing work on a computer. Remember, once it is the

4

ALWAYS ask permission from a teacher before using the internet.

5

NEVER use gaming websites, social networking or an internet chatroom in school. **NEVER** upload or download any files

6

When using the internet or e-mail, **NEVER** give any personal details (name, address, phone number, school, e-mail address) or arrange to meet someone.

7

ALWAYS then tell an adult straight away if you see anything that makes you feel uncomfortable.

8

NEVER change any of the settings on the computers or iPads unless asked to by an adult.

9

ONLY print if you have been given permission.

10

ALWAYS report any damage to the computer equipment to an adult. **ALWAYS** carry equipment with two hands.

IF YOU BREAK THESE RULES YOU MAY BE STOPPED FROM USING THE COMPUTERS

Appendix 5: Staff Self-Check List

Internet

- My children know that should they find a web page that upsets them they are to turn off the monitor and see me immediately.
- I know the procedure for reporting offence material on a website.
- I understand that no pupil can use the internet without supervision, particularly at wet plays or lunch times.
- I will only use the Internet, ICT equipment or other technologies according to school policy and within clear and explicit professional boundaries. The consequences of any breach of trust could lead to me being banned from working with children and possible legal proceedings

E-mail

- I check children's school e-mail accounts/ VLE messenger as appropriate to ensure that they are used in a safe, purposeful and appropriate manner.
- I will only communicate with children through the school VLE and in accordance with school policy and within clear and explicit professional boundaries
- I will only use school email accounts for school communications.
- I will not contact parents through my school email address or my personal address.
- I will not send any personal information via my personal email address.

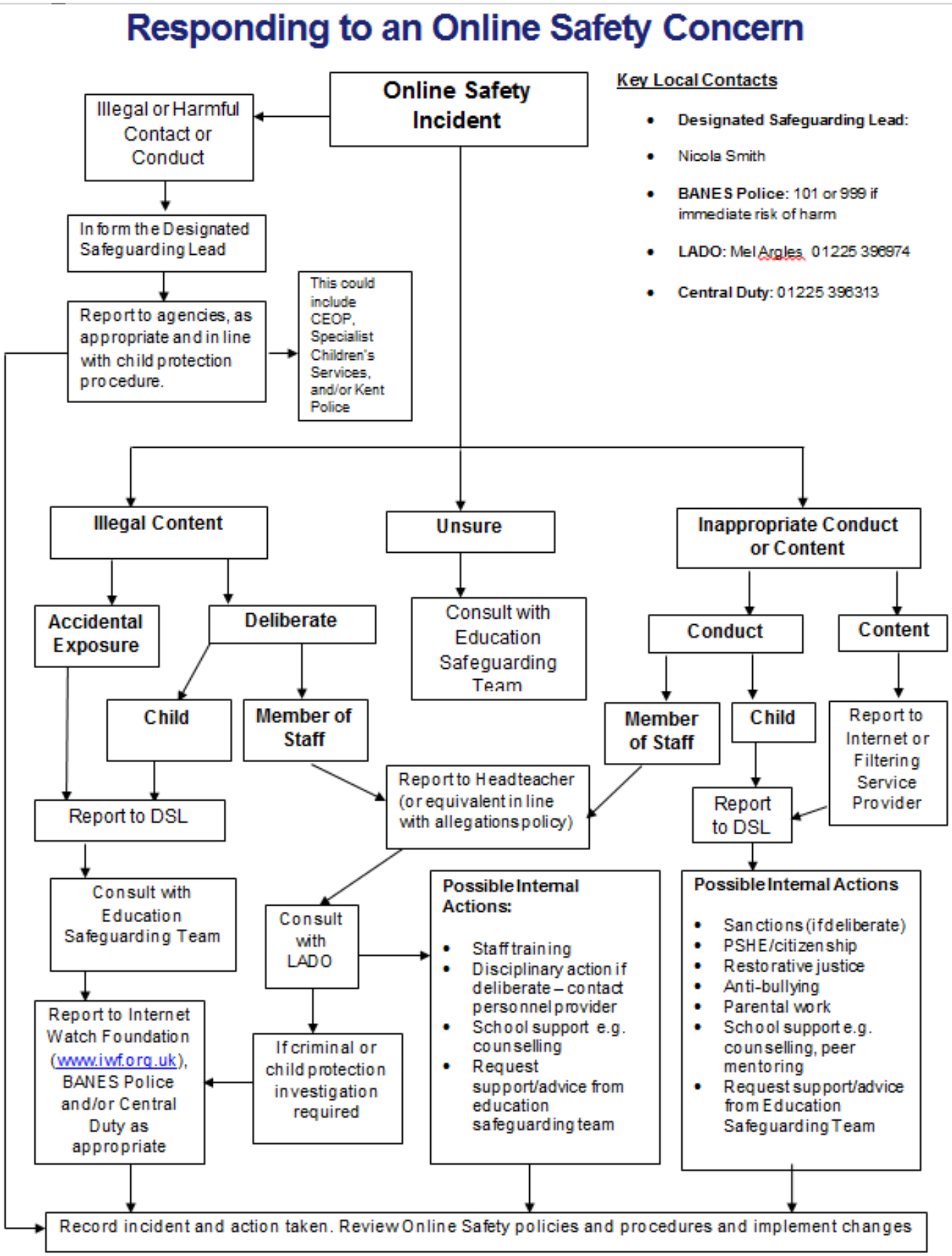
Other Technologies

- I will save digital photographs into a class picture folder on the school server.
- I will delete images from the class iPad as soon as I have downloaded them to the school server.
- I will turn off photo sharing on the iPad to avoid images being shared with all iPads.
- I will not identify individuals when uploading onto the school website.
- I will only record images with due regard to the law and the need to safeguard the privacy, dignity, safety and wellbeing of children.
- I will check the schools picture permission and understand that this means that there is informed written consent from parents or carers and agreement where possible from the child.
- I will avoid images in one to one situations or which show a single child with no surrounding context.
- I know it is NOT appropriate for any adult to take photographs of children for their personal use. I will report any concerns I have about inappropriate or intrusive photographs I find.
- I will not use mobile phones or personal devices to take images of children.
- I will model the acceptable use of mobile phones and other technologies.
- I will not take images in 'secret' or in any situation which may be construed as 'secretive'.
- I have read and understood the Internet and Online Safety Policy.
- I have signed, returned and taken note of the Acceptable Use (Internet / Associated Technologies) Agreement (Staff & Adults).

Appendix 6: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 7: Responding to an Online Safety Concern



Appendix 8: Useful Websites

- UKCCIS Guidance for Schools

  https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
- Key Documents For Schools from Karl Hopwood

  http://www.esafetyltd.co.uk/
- LSCB E Safety Strategy

  http://www.bathnes.gov.uk/sites/default/files/sitedocuments/Children-and-Young-People/ChildProtection/e-safety strategy_june_2016.pdf
- UK Council for Child Internet Safety (UKCCIS)
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/562876/Guidance_for_School_Governors_-_Question_list.pdf
- Somerset Learning platform

  http://bit.ly/elimsomersetpolicies
- South West Grid for Learning

  http://www.swgfl.org.uk/Staying-Safe
- SWGFL Policy template

  http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates
- Online Safety FAQs

  http://swgfl.org.uk/FAQs/Online-Safety-FAQs
- 360 Degree Safe

  https://360safe.org.uk/
- 360 Degree Safe self-review tool (free)

  https://360safe.org.uk/About-the-Tool
- Childnet; including Cyberbullying and Filtering guidance

  http://www.childnet.com/

  www.childnet.com/cyberbullying-guidance

  http://www.childnet.com/blog/appropriate-filtering-and-monitoring-required-in-schools-from-5th-september
- Kidsmart

  http://www.kidsmart.org.uk/
- Digital Parenting Magazine

  http://www.theparentzone.co.uk/vodafone_digital_parenting_magazine/2248_0
- Internet Matters (for parents)

  www.internetmatters.org
- NSPCC – Net Aware

  http://www.net-aware.org.uk
- Think You Know

  www.thinkuknow.co.uk
- Safer Internet Helpline

  www.saferinternet.org.uk/about/helpline