St Nicholas School

Online Safety Policy

St. Nicholas School Canterbury

Policy Created	**December 2022**
Governing Body Committee	**LCS Committee**
SLT responsibility	**David Jenner**
Date Reviewed by Governing Body	**Adopted by Chairperson's Action on 20/4/23**
Date of Next Review	**December 2023**

ONLINE SAFETY POLICY (INC. GUIDANCE ON THE USE OF SOCIAL AND DIGITAL MEDIA)

INTRODUCTION

This policy was developed by the Curriculum Co-ordinator for Information and Communications Technology (ICT) in consultation with the whole teaching staff and following guidelines provided by the KCC Online Safety policy and from government. This policy has been agreed by the Senior Leadership Team and has been approved by the Governing Body. It is reviewed annually.

This policy must be considered in conjunction with other subject policies, as ICT, Safeguarding, Behaviour
/ Anti-bullying and PSHE & Citizenship. It is considered a core area of provision for 'Staying Safe' across the whole school curriculum. The school has appointed Stephen King the Online Safety Coordinator as he is a Designated Safeguarding Lead and a CEOP/NCA ThinkUKnow Ambassador for Online Safety Training. The Computing Curriculum Manager also is a CEOP ThinkUKnow trainer (who assists in the co-ordination of Online Safety schemes of work). The school is registered with the 360° Safe Online Safety programme and has achieved the Certificate of Progress; it is seeking to complete the Online Safety Mark in the near future. All class teachers undergo the CEOP ThinkUKnow Online Safety training, as part of the schools' aim to ensure excellence in the teaching of Online Safety to all pupils as part of their ICT, Computing and PSHE cross-curricular education.

St. Nicholas School has appointed an Online Safety Co-ordinator (and CEOP Ambassador) who assumes responsibility for Online Safety issues and training in-school, at home school and in the local community. Staff and students have a responsibility to report any Online Safety (including Cyberbullying) concerns in and out of school. The school promotes Online Safety in partner schools in the locality, enabling release time for the ThinkUKnow trainer to work on all partner campuses and / or local mainstream schools.

Heidi Dawson is the named Online Safety governors who liaise with the Headteacher and ICT/ Online Safety Co-ordinator on a regular basis. The school has established an Online Safety Committee made up of SLT, Governor, pupils, class teaching and support staff who meet to review policy, practices and procedures. Online Safety matters are considered of the highest importance for our staff and pupils; Online Safety is addressed through classroom lessons - PSHE, ICT and discrete Online Safety sessions and assemblies, as appropriate. The School has an Online Safety Committee which meets twice in the year – it involves the Online Safety Co-ordinator, Governors, ICT Systems staff and a group of pupils from the school council.

PURPOSE

The Kent PSCN School consortium believes that the Internet is an invaluable tool for the following reasons:

To share expertise in the quality of teaching and learning of pupils with Profound, Severe and Complex Learning Difficulties; to enhance links with the local community; to strengthen communication across the consortium in all areas of school life; to enhance the ability of the pupils to communicate and provide them with a powerful tool and aid life skills and to enhance pupils' access to the National Curriculum and the wider curriculum.

St. Nicholas School believes that:

- Online Safety (e-Safety / Online Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- St. Nicholas School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- St. Nicholas School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- St. Nicholas School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.
- The purpose this Online Safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that St. Nicholas School is a safe and secure environment.
    - Safeguard and protect all members of our school community online.
    - Raise awareness with all members of our school community regarding the potential risks as well as benefits of technology.
    - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
    - Identify clear procedures to use when responding to Online Safety concerns that are known by all members of the community.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, Acceptable Use Policies (inc. Internet / Technology Use, Image Use, Social Media Use, Mobile Technology and Wi-Fi Use - see appendices A - D), confidentiality, and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

POLICY INTO PRACTICE

Key Responsibilities

Senior Leadership Team:

- Developing, owning and promoting the Online Safety vision and culture to all stakeholders,

in
line with national and local recommendations with appropriate support and consultation throughout the school community.

- Ensuring that Online Safety is viewed by the whole community as a safeguarding issue and proactively developing a robust Online Safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their Online Safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding Online Safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology (see Appendix A).
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding Online Safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that Online Safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of Online Safety and the associated risks and safe behaviours.
- To be aware of any Online Safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding Online Safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting Online Safety.
- Auditing and evaluating current Online Safety practice to identify strengths and areas for improvement.
- To ensure that the Designated Safeguarding Lead (DSL) works with the Online Safety lead.

Designated Safeguarding Lead / Deputy DSLs:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding Online Safety.
- Coordinating participation in local and national events to promote positive online behaviour,
  e.g. Safer Internet Day.
- Ensuring that Online Safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of Online Safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms
- Monitor the schools Online Safety incidents to identify gaps/trends and use this data to update the schools education response to reflect need
- To report to the school management team, Governing Body and other agencies as appropriate, on Online Safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school leadership and management to review and update the Online Safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that Online Safety is integrated with other appropriate school policies and procedures.
- Leading an Online Safety team/group with input from all stakeholder groups.
- Meet and / or liaise regularly with the governor with a lead responsibility for Online Safety.

All Staff members:

- Contributing to the development of Online Safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them (see Appendices A-D).
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different Online Safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding Online Safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate Online Safety issues, internally and externally.
- Being able to signpost to appropriate support available for Online Safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

- **ICT Systems Management Staff:**
- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.

- Ensuring that the use of the School's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate Online Safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

The key responsibilities of children and young people are:

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

- At a level that is appropriate to their individual age, ability and vulnerabilities:
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

The key responsibilities of parents and carers are:

- Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing Online Safety issues with their children, supporting the school in their Online Safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school Online Safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the

opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The ICT Curriculum Manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Email addresses will be published carefully online, to avoid being harvested for spam.
- Pupils work will be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including Online Safety, on the school website for members of the community.

2.2 Publishing images and videos online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- The school will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

- Pupils may only use school provided email accounts for educational purposes
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work life balance when

responding to email, especially if communication is taking place between staff and pupils and parents.

- Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- The Online Safety Manager (Deputy Headteacher) will be made aware of any and all inappropriate content or language used in school-based emails – EIS will forward a copy of any offending emails (detected by their protection systems) to the Online Safety Manager, who will manage the incident as a behavioural concern (if pupils are involved), a disciplinary matter (if staff are involved) or Safeguarding incident (if required).

2.4 Official videoconferencing and webcam use for educational purposes

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

Users

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

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet and any associated devices

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

3. All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place. The school has entered all and laptop computers (including Windows Tablets) onto the school curriculum network so that not only can they be synched / backed up to the school network and MS OneDrive Cloud service, but be monitored for content and usage e.g. via the Lightspeed SSL Proxy Sever – which will block suspicious internet searches in real-time and send a daily report to the school. It is intended that school I-pad use will be monitored by MDM monitoring and mobile device management software.

4. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.6 Management of school learning platform

- Leaders/managers and staff will regularly monitor the usage of the Kent Learning Zone (KLZ) Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the LP 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.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Social Media Policy

3.1. General social media use (See Appendix C – Acceptable Social Network Use)

- Expectations regarding safe and responsible use of social media will apply to all members of the St. Nicholas School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and

many others.

- All members of the community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the community via regular Online Safety training updates, the school website, newsletter, text system and via the school official PTFA Facebook (closed) group.
- 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 or call into question their professional judgement or potentially cause reputational damage to the school.
- The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems – with the only permitted social network being used by / with pupils being the Edmodo (school / education-based) Social Network.
- The use of social networking applications on the main school-site is not permitted. For satellite or off-site provisions the use of social networking, although possibly permitted by their internet systems, is not permitted for any pupil. Staff may be allowed to use the system but our staff may only do so out of school hours.
- 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. Staff may not use their own mobile devices to access social media during school hours. Any publishing of school events or activities may only take place on the school website or via the official school PTFA Facebook (closed) group.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour, Staff Code of Conduct and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

- The St. Nicholas School official social media channels are:
  - PTFA Closed Facebook Group – https://www.facebook.com/groups/744976165568740/
  - Twitter Feed – https://twitter.com/SchoolNicholas
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed

and formally approved by the headteacher.

- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation – see Appendix C: Acceptable Social Media Use.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where appropriate, linked to from the school website and take place with written approval from the Leadership Team – the school PTFA Facebook page is a closed group which needs authorised approval to join.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and l action taken to safeguard the community.
- Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3: Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including

volunteers) as part of the school Acceptable Use Policy and link to the personal behaviour elements of the Staff Code of Conduct and Confidentiality policies.

- All members of staff are prohibited from communicating with or adding as 'friends' any current or past children/pupils, nor are they allowed to contact them via mobile phone or any other digital media as this would contravene our Safeguarding and Staff Code of Conduct Policies. Staff are strongly advised to contact or add as 'friends', communicate with any family members of our current pupils, any past pupils or their family members via any personal social media sites, applications or profiles. Staff are advised not to contact via their own mobile phones or any other digital media. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead (Headteacher) and/or the Deputy Headteacher (Online Safety Manager). If staff do not follow the advice of this policy and do maintain digital or social media with parents or past pupils, the school cannot support staff with any potential issues that this unofficial contact may cause.

- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels (using official school provided email address or phone numbers).
- Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead or Online Safety manager.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites. Staff are prohibited from sharing information about or publishing photographs of school events / taken on the school premises.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential. Staff are aware that their social media posts reflect on them personally and professionally so they are advised to think before they post. Staff will not be able to be supported by the school if their social media profile calls their professional judgement or reputation or the reputation of the school into question.
- 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 (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework. Staff are aware that their social media posts reflect on them personally and professionally so they are advised to think before they

post. Staff will not be able to be supported by the school if their social media profile calls their professional judgement or reputation or the reputation of the school into question.

- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership and Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- Members of staff are prohibited from identifying themselves as employees of the school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community. Staff are encouraged not to allow their posts or photographs to identify them as an employee of the school.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media, including official school social media channels.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow or 'like' the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries and act professionally on these platforms, particularly if joining using a personal account.

3.4: Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead (Headteacher) and/or the Deputy Headteacher (Online Safety Manager) of any concerns such as inappropriate content or criticism of the school,

its staff or its policies and practices posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will sign the school social media Acceptable Use Policy.

Pupils use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes e.g. using the Edmodo programme.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Pupils will be encouraged to report anything they see, hear or experience online that concerns, worries or scares them to a parent/carer or school staff member – 'Always remember to tell someone!'
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour and be reported via an Online Safety Concern form or the school 'green' safeguarding concern form.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

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

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies (see the list above).
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in within the school buildings, but, in specific areas such as changing rooms, toilets and hydro pool – this will be considered a safeguarding risk and become a disciplinary issue. (School leaders and other
  members of staff given permission by the SLT may use a mobile phone in the main school / SLT office areas).
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Code of Conduct and / or Positive Behaviour Support policies.
- Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required. In exceptional circumstances, staff may be given permission to use their personal mobile phones but advice will be given as to how their phone number will be anonymised. Staff are not given permission to share their own personal mobile number with parents/carers (unless in very exceptional circumstances and with the permission of the SLT).
- All members of the school community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the school community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the school community will be advised to ensure that their mobile

phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.
- School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies (see above).
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use and mobile phone policies.
- Pupil's personal mobile phones and personal devices, if allowed by the classteacher (in agreement with SLT) will be switched off during lessons – should the use of pupil mobile phones cause a disruption or behavioural incident, permission for the pupil/class to bring in or use their phones may be withdrawn.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff, in conjunction with the SLT. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted. If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Leadership Team.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the SLT.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examination setting. Pupils found in possession of a mobile phone or personal device during an exam or controlled assessment will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy then the phone or device will be confiscated by a member of the SLT and will be held in a secure place in a school office. Mobile phones and devices will be released to parents/carers in accordance with the school mobile phone policy.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour / anti-bullying policies or could

contain (youth produced sexual imagery / sexting) i.e. sharing or nude or semi-nude images. The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the school' safeguarding and acceptable use policies. https://www.gov.uk/government/publications/searching-screening-and-confiscation

- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.5 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children or young people within or outside of the setting in a professional capacity. Staff are not permitted to communicate with the parents / carers / families (unless in specific and exceptional circumstances, with the permission of the SLT). Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose (unless in specific circumstances and with the permission of the SLT – see acceptable image use policy Appendix B).
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. Confidentiality, Data Protection, Acceptable Use, Staff Code of Conduct etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school whistleblowing policy.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school acceptable use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use i.e. the use of phones or 3G/4G internet is not permitted on school grounds.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos of special school must take place in accordance with the school image use policy and inappropriate use of this may result in the withdrawal of this opportunity / exception.

5. Policy Decisions

- St. Nicholas School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content i.e. Kent Public Service Network Internet Service Provider with Lightspeed filtering system & SSL Proxy Server and internal network monitoring and additional filtration via MDM – a triple protection lock.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the Online Safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.
- If staff wish to use their own devices to access their work files or emails they will need to ensure that they have adequate data security and protection software on each device. The school operates a Bring Your Own Device To Work Policy (see Staff Code of Conduct Policy) and have declared their aim to use this opportunity to the Senior Leadership Team, on an annual basis.
- Sensitive personal information or data files may only by saved or transported using encrypted cloud or USB storage areas.

5.2. Internet use throughout the wider school community

- The school will liaise with local organisations to establish a common approach to Online Safety.
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site, including the guest Wi-fi network (see Appendix D – Acceptable Wi-Fi Use policy.

5.3 Authorising internet access

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

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An Online Safety (e-Safety/Online Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils input will be sought when writing and developing school Online Safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online Safety (e-Safety/Online Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use.
- Online Safety (e-Safety/Online Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- All teachers will be able to support pupils in their learning, safety / protection and

decisions regarding Online Safety as they are CEOP/NCA ThinkUKnow Trainers. The Online Safety Manager is a CEOP/NCA Ambassador and regional Trainer trainer.

- External support will be used to complement and support the schools internal Online Safety (e- Safety) education approaches e.g. the CEOP ThinkUKnow / Kent e-Safety Safer Online resources.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop Online Safety as appropriate to the needs of the pupils.

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

- St. Nicholas School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- We will ensure that differentiated and ability appropriate Online Safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. Online Safety Manager, Creative Therapists, DTCiC).

6.3 Engagement and education of staff

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

6.4 Engagement and education of parents and carers

- St. Nicholas School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school Online Safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.

- A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting Online Safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read Online Safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Full information regarding the schools approach to data protection and information governance can be found in the schools Data Protection and Security Policy.

7.2 Security and Management of Information Systems

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

7.2a Password policy

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

- All pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We expect staff and pupils to change their passwords on a regular basis.
- The admin passwords are kept under lock and key.

7.3 Filtering and Monitoring

Extract from the St. Nicholas School Child Protection Policy 2023

- St. Nicholas School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems and will ensure that appropriate filtering and monitoring systems are in place. Our filtering and monitoring (F&M) system provides a solution that not only meets the needs of our school and our staff / students (with SEND) it also fully meets the requirements of both Keeping Children Safe in Education 2023 and the DFE Filtering and Monitoring Standards for schools. The school reviews our provision of F&M (at least annually) using the South West Grid for Learning 360° Safe platform – dave?. The F&M system blocks harmful and inappropriate content, in real-time, and does not unreasonably impact on teaching at learning.
- The following 3 roles and responsibilities have been identified and assigned as part of our statutory duties to have an F&M team –
    1. F&M leader – Stephen King (DSL)
    2. F&M curriculum manager – David Jenner (Online Safety and Computing Co-ordinator)
    3. F&M technical manager – Matt Arnold (ICT Systems Manager).
  - The F&M technical manager is responsible for checking and responding to any attempted breaches of the filtering system and this is recorded in a monitoring log. The F&M team make a shared decision as to what would constitute inappropriate and harmful content, they also check that the system is up-to-date. The F&M leader receives notifications about the potential use of inappropriate search words. The F&M leader also receives notifications in real-time of the use of words that do not fail to meet the lexicon of approved words for the profanity filter of our email service provider. All staff understand from training and daily practice that they are all responsible for being vigilant in their monitoring and supervision of pupils' and colleagues' using of email communication, internet search terms and use of the ICT systems. NB: although the use of mobile internet technology is not allowed on the school grounds, all staff have a responsibility to monitor the use of (pupils and / or colleagues) personal devices if present to ensure that safe F&M duties can be applied to devices not directly connected to the school ICT systems.

  - The school uses Lightspeed Relay for website filtering for staff and students. This included monitoring, reporting and access to websites. We carried this filtering solution over from our previous suppler of email and broadband services, in order to maintain 'like for like' services as part of that transition.
  - Microsoft 365 is the platform we use that contains tools for communication. Email, Teams and Onedrive are part of this. There are tools for monitoring, reporting and access to these services via the Microsoft 365 platform. We have this platform courtesy of Microsoft who offer Office 365 services free to schools, which has replaced our older segregated services of email and communication software (Skype)
  - These system are being secured through tools included with both lightspeed and Microsoft 365 platform. On computers directly, we also use 3rd party antivirus/malware protection through Trent Micro Antivirus. Ongoing training and advise is offered to all staff to help prevent phishing/social engineering scams.
    - If learners or staff discover unsuitable sites or material, they are required to: turn off monitor/screen (where possible), report the concern immediately to a member of staff who will report the URL of the site to the ICT team.
    - All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation.
    - Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to the DSL who will respond as appropriate.

- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the Internet Watch Foundation and the police.
- When implementing appropriate filtering and monitoring, St. Nicholas School will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

- St. Nicholas School acknowledges that whilst filtering and monitoring is an important part of school internet safety responsibilities, it is only one part of our approach to internet safety.
  - Learners will use appropriate search tools, apps and online resources as identified following an informed risk assessment.
  - Learners internet use will be supervised by staff according to their age and ability.
  - Learners will be directed to use age appropriate online resources and tools by staff.

- The governing body will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks. The school has 2 Safeguarding Governors who oversee Online Safety.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils
- The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will work with KCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of – to inform the DSL, ICT Systems management team, Online Safety Manager or Computing manager immediately.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- Network monitoring (and additional filtration) will be provided by the ICT Systems Management team and – the triple lock system of Lightspeed, KPSN and SSL Proxy Server systems.
- All changes to the school filtering policy will be logged and recorded.

- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.
- The Online Safety Manger (Deputy Headteacher) will be forwarded a copy of the details of any inappropriate Internet Use, as detected by EIS / KPSN systems (inc. Lightspeed SSL Proxy server) or the school MDM system – incidents involving pupils will be dealt with as a behavioural matter, those involving staff will be a disciplinary matter.

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

- The headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images (unless in exceptional circumstances and in agreement by the SLT and then removed permanently from the device).
- Laptop devices and USB sticks used by teachers will be appropriately encrypted, so that if they are taken off site, a data security breach will be prevented in the event of loss or theft – see Data Protection Policy. No unencrypted device will be allowed to save any personal information locally on a hard disk – the information will be stored on their encrypted and secure Office 365 OneDrive cloud account (TPM encrypted laptops will be allowed to download and save files to their machine's OneDrive synching folder).
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including nudes / semi-nudes ('sexting' images), online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting Online Safety (e-Safety) concerns, such as breaches of filtering, nudes/semi-nudes, cyberbullying, illegal content – report the concern to the Online Safety Manager or on-call DSL who will record the incident on an Online Safety concern form (or green safeguarding concern form if it is serious enough to become a safeguarding incident).

- The Designated Safeguarding Lead (DSL) will be informed of any Online Safety (e-Safety) incidents involving child protection concerns, which will then be recorded – as described above.
- The DSL will ensure that Online Safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- All Online Safety, bullying (including cyberbullying) and racial incidents are discussed at the weekly Safeguarding review meeting.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedures.
- Any complaint about staff misuse will be referred to the head teacher or on-call SLT member.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will be made aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage Online Safety (e-Safety) incidents in accordance with the school discipline / behaviour policy where appropriate.
- The school will inform parents / carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent.
- Parents and children will need to work in partnership with the school to resolve issues.

9 Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding the sharing of Nude or Semi-Nude Images (Youth Produced Sexual Imagery or "Sexting")

- St. Nicholas School ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating nudes / semi-nudes - youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers including the CEOP ThinkUKnow resources, using the support of the local PSCO and Community Safety Officer etc.
- St. Nicholas School views sharing nude / semi-nude images as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance.
    - If the school are made aware of incident involving creating youth produced sexual imagery the school will:
        - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
        - Immediately notify the designated safeguarding lead.
        - Store the device securely.
        - Carry out a risk assessment in relation to the children(s) involved.
        - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
        - Make a referral to children's social care and/or the police (as appropriate).
        - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
        - Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
        - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
        - Inform parents/carers about the incident and how it is being managed.
        - The school will not view an images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
        - The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
        - If an indecent image has been taken or shared on the school network or

devices then the school will take action to block access to all users and isolate the image.
    - The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
    - The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

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

- St. Nicholas School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- St. Nicholas School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DSL.
- If the school are made aware of incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the

use of school equipment or personal equipment, both on and off the school premises.

- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and all other members of the school community, as it is embedded on the school website's "Learning Wall".

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

- St. Nicholas School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect

images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. The school monitors the use of the School Network themselves and the use of I-pads onsite via MDM. All internet traffic and searches is constantly monitored by the KPSN SSL Proxy Server.
- The Online Safety Manger (Deputy Headteacher) will be forwarded a copy of the details of any Internet use and information searches, as detected by EIS / KPSN systems or the school MDM system – incidents involving pupils will be dealt with as a behavioural matter, those involving staff will be a disciplinary matter.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy – completing the school safeguarding form and indicating an extremism concern.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police. Pupils may be referred to the Channel Panel, if appropriate, in an attempt to support their de- programming and de-escalate their radicalisation.

9.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the St. Nicholas School community will not be tolerated. Full details are set out in the school policies regarding anti- bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools Online Safety (e-Safety) ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti- bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

9.6 Responding to concerns regarding online hate

- Online hate at St. Nicholas School will not be tolerated.
- All incidents of online hate reported to the school will be recorded as Racial and / or Bullying Incidents.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc. Those involving pupils will be reported via the KCC online Bullying and Racial Incident reporting system.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

10. ONLINE SAFETY FOR STAFF AND PUPILS

HOW WILL THE POLICY BE INTRODUCED TO

PUPILS?

- Rules for Internet access will be posted in all rooms where computers are used.
- Pupils will be informed that internet and network use will be monitored
- An Online Safety training programme is established across the school to raise the awareness and importance of safe and responsible Internet use. The training should precede individual Internet access.
- The policy will be discussed at school council meetings, as part of the AIU policy statement review (see appendix A).
- The policy will be shared via PSHE, ICT and discreet Online Safety lessons (see scheme of work).

HOW WILL STAFF BE CONSULTED?

- All staff must accept terms of the 'Acceptable Internet and Equipment Use' statement before using any internet resource in school.
- All staff including teachers, supply teachers, supply staff, classroom assistants and support staff, will be provided with the Online Safety Policy, and its importance explained via the induction pack and training session, when joining the school. Updates to this policy will be delivered by explicit Online Safety training (an annual option), at teachers' meetings and / or via the whole-school Staff Training Meeting, once per year.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user by the Network Manager. Discretion and professional conduct is essential. Any such monitoring will be conducted by the Senior Management Team.

HOW WILL PARENTAL SUPPORT BE ENLISTED?

- Parents' attention will be drawn to the School Internet Policy in newsletters, the Acceptable Internet and Equipment Use statement, the school prospectus and via the school Website. A copy of this policy and the 'Acceptable Use of Internet and Equipment Statement' will be provided to all new parents on admission to the school. Also provided at this time will be the permission for pupils to be included in photographs, videos and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This may include demonstrations, practical sessions and suggestions for safe Internet use at home.

MONITORING AND REVIEW

The school Online Safety Committee featuring the named Online Safety governor (Heidi Dawson), pupils, teaching and support staff meet on a twice-yearly basis to discuss Online Safety - policy, concerns, Scheme of Work and other issues. This policy and the provision will be monitored on a yearly basis by the Curriculum Co-ordinator along with the Online Safety Manager (using the Schools Online Safety Audit Tool) - See appendix E) to keep up to date with any adjustments to statutory legislation or curriculum and any changes will go via the Governing Body when necessary.

EQUALITY, SAFEGUARDING AND EQUAL OPPORTUNITIES STATEMENT

St Nicholas School, in all policies and procedures, will promote equality of opportunity for students and staff from all social, cultural and economic backgrounds and ensure freedom from discrimination on the basis of membership of any group including gender, sexual

orientation, family circumstances, ethnic or national origin, disability (physical or mental), religious or political beliefs.

As part of our commitment to meet the Public Sector Equality Duty (PSED), St Nicholas School aims to:

- Provide equal opportunity for all;
- Foster good relations, and create effective partnership with all sections of the community;
- Only take actions which does not discriminate unlawfully in service delivery, commissioning and employment;
- Provide an environment free from fear and discrimination, where diversity, respect and dignity are valued.

All aspects of Safeguarding will be embedded into the life of the School and be adhered to and be the responsibility of all staff will be embedded into the life of the school and be adhered to and be the responsibility of all staff.

LINKS TO OTHER POLICIES

ICT Policy / Acceptable Use Policies
Website Management Policy
Anti-Bullying Policy
Child Protection Policy
Health and Safety Policy
Positive Behaviour Support Policy
Teaching and Learning Policy
Staff Code of Conduct Policy
All Curriculum Subject Policies

Appendix E - Schools Online Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for Online Safety policy. Staff that contribute to the audit include: Designated Child Protection Coordinator, SENCO, Online Safety Coordinator, Network Manager and / or Head Teacher.

Does the school have an Online Safety Policy that complies with Kent guidance?		Y/N
Date of latest update:	Date of future review:	
The school Online Safety policy was agreed by governors on:		
The policy is available for staff to access at:		
The policy is available for parents/carers to access at:		
The responsible member of the Senior Leadership Team is:		
The governor responsible for Online Safety is:		
The Designated Safeguarding Lead is:		
The Online Safety Coordinator is:		
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the		Y/N

school Online Safety Policy?	
Has up-to-date Online Safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	Y/N
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an Online Safety incident of concern?	Y/N
Have Online Safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is Online Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are Online Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers or pupils sign an Acceptable Use Policy?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the school log and record all Online Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school Online Safety policy and ethos on a regular basis?	

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

Kent Support and Guidance
Kent County Councils Education Safeguards Team:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
Kent Online Safety Support for Education Settings

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police: www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-

urgent enquiries contact Kent Police via 101
Kent Public Service Network (KPSN): www.kpsn.net
Kent Safeguarding Children Board (KSCB): www.kscb.org.uk
Kent e–Safety Blog: www.kentesafety.wordpress.com
EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources
Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF):
www.iwf.org.uk **Lucy Faithfull Foundation:**
www.lucyfaithfull.org **Know the Net:**
www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk **NSPCC:** www.nspcc.org.uk/onlinesafety
Professional Online Safety Helpline:
www.saferinternet.org.uk/about/helpline **The Marie Collins**
Foundation: http://www.mariecollinsfoundation.org.uk/ **Think U**
Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/