St Nicholas Church of England Primary School

E-Safety Policy and Acceptable Use Policies

Review date: October 2023

1. E-Safety Policy – Responsibilities

All members of staff at St Nicholas are responsible for e-safety. All staff are supported by our computing lead, Designated Safeguarding Leads (DSLs) and their deputies. Our ICT technician is also consulted when required.

DSL – Mrs Alison Shearer and Mrs Alecia Spike

Computing lead – Mr Chris Pavey

The DSLs are responsible for ensuring our computing lead organises and/or delivers staff training when needed and at regular periods throughout each school year. Recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety with St Nicholas are our top priorities. Our computing lead will also be required to deliver workshops for parents/guardians.

AUPs – internet use and Acceptable Use Policies

All members of our school community should agree to an Acceptable Use Policy that is appropriate to their age and role.

Examples of the AUPs used here at St Nicholas can be found in appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter and reply slip. The can be found in appendix 2.

AUPs will be reviewed annually. All AUPs will be stored centrally in case of breaches of the e-safety policy.

The AUP will from part of the first lesson of Computing for each year group.

2. **The Prevent Duty**

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities – schools – in the exercise of their functions, to have due regard to the need to prevent people from being drawn in to terrorism. The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an extremely important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in school. Schools should ensure that suitable filtering in in place. At St Nicholas, this is checked by our ICT technician.

More generally, schools have an important part to play in equipping children and young people to stay safe online, both in school and outside of school. Internet safety will be integral to our ICT curriculum and can also be embedded in PSHE and SRE (sex and relationships education.)

General advice and resources for schools on internet safety are available on the NSPCC website. As with other online risks of harm, all staff need to be aware of the risks posed by online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and, where necessary, report concerns over the use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals.

The Prevent Duty requires a school's mentoring and filtering systems to be fit for purpose.

3. **Photographs and Video**
   The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents or guardians is gained if videos or photos of pupils are going to be used. If photos/videos are to be used, then names of pupils should not be linked to pupils. Staff must be fully aware of the consent form responses from parents when considering the use of images. This is updated annually as part of the data collection exercise. Staff should always use a school camera to capture images and should not use their personal devices.

4. Photos and Videos taken by parents/guardians
   Parents and guardians are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos

from school events on social networking sites if other pupils appear in the background. Parents attending school-based events will be reminded, both verbally and through text messages/notices, of their responsibilities in relation to social media.
The parental letter concerning AUPs includes a paragraph concerning posting photos on social networking sites – see appendix 2.

Photos for personal use such as those taken by parents/guardians are not subject to the Data Protection Act.

5. **Mobile Phones and Other Devices**

St Nicholas C of E Primary School recognises that staff may need to have access to mobile phones on site during working hours. Staff should not be checking their phone in any way during teaching hours. Phone checking can be done during non-contact time. Any exceptional circumstances must be discussed with the Headteacher. If a staff member is expecting a phone call, then they are to provide the caller with the school office phone number so that class/duty cover may be correctly organised in an appropriate manner.

6. **Ensuring safe and appropriate use of mobile phones.**

Staff are allowed to bring their personal phones to school for their own use but will limit such use to non-contact time when pupils are not present. Staff members' personal phones will remain in their bags or cupboards during contact time with pupils.
Staff will not take photographs or recordings of pupils on their personal phones or personal cameras.
We will follow the General Data Protection Regulation and Data Protection Act 2018 when taking and storing photos and recordings for use in our school. Cameras tablets are used across the school to capture activities. These photos or videos are for assessment purposes only and remain the property of St Nicholas.
If staff fail to follow this guidance, disciplinary action will be taken in accordance with the school's staff code of conduct.
When individual cases are discussed and agreed with the Headteacher and the parent/guardian, children may be allowed to bring their personal phone to school – eg, older pupils walking to and from school. However, the pupils are not allowed to use personal phones during school hours or

have them in their bags, classroom or playground. Phones must be handed in to the school office at the beginning of the school day and collected at the end of the school day. If a pupil uses their personal phone during school hours, the phone will be confiscated.

7. **Use of mobile phones for volunteers and visitors**

Upon their initial visit, volunteers and visitors are given safeguarding information – our St Nicholas's signing in to school record sheet is only completed once each visitor/volunteer has read the safeguarding information. Their signature is evidence that they have read and fully understood what our school's expectations are in relation to safeguarding. This information sheet informs them that they are not permitted to use mobile phones on our premises. If they wish to make or take an emergency call, they may use the main line in our school office or the one in the Head teacher's office. No volunteers or visitors are permitted to take photographs or recordings of the children without the Head teacher's permission.

At St Nicholas, we believe that photographs validate children's experiences and achievements – they are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at St Nicholas. We take a mixture of photos that reflect the pre-school environment. Sometimes, this will be when children are engrossed in an activity either on their own or with their peers. Children are encouraged to use the camera to take photos of their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken in to the toilets by adults or children. All adults, whether teachers, support staff or volunteers at St Nicholas, fully understand the difference between appropriate and inappropriate sharing of images. All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within St Nicholas, then it should be confiscated – staff should not 'search' the phone. The incident should be passed directly to the Head teacher/DSL – designated safeguarding lead who will liaise with our Computing Lead.

8. **Use of E-mails**

Pupils should only use e-mail addresses that have been issued by St Nicholas – this e-mail system should only be used for school related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

9. **Security and passwords**

Passwords should be changed regularly and must not be shared. Staff must always 'lock' the work station if they are going to leave it unattended.

All users should be aware that the ICT system is filtered and monitored.

10. **Data Storage**

Only encrypted USB pens are to be used. No other. Staff are advised to use the shared google drive for all documents.

11. **Reporting**

All breaches of the e-safety policy need to be recorded. The details of the user, date and incident should be reported. Incidents which lead to child protection issues need to be passed on to the DSL immediately – it is their responsibility to decide on what appropriate action is taken; this is not for class teachers to decide.

Incidents that are of a concern under the Prevent Duty should be referred to the DSL immediately. The DSL will decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention, for example cyberbullying, should be reported to the members of staff at the school responsible for e-safety on the same day; this is most likely the Head teacher or our Computing lead teacher.

Allegations involving staff must be reported to the Head teacher. If the allegation is one of abuse, then it should be handled according to the DFE document entitled 'Dealing with allegations of abuse against teachers and other staff.' If necessary, the LADO from the local authority should be informed. Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents – eg ChildLine / trusted adult / NSPCC.

12. Infringements and sanctions

When a pupil infringes the e-safety policy, the final decision on the level of sanction will be at the discretion of the St Nicholas leadership team. The following are provided as exemplifications only:

Level 1 infringements:

- **Use of non-educational sites during lessons**
- **Unauthorised use of e-mail**
- **Use of unauthorised instant messaging/social networking sites**

Possible sanctions = referred to the class teacher / Head teacher / DSL + confiscation of phone.

Level 2 infringements:

- **Continued use of non-educational sites during lessons after being warned**
- **Continued unauthorised use of e-mail after being warned**
- **Unauthorised use of mobile phones or other new technologies**
- **Continued use of unauthorised instant messaging/social networking sites**
- **Use of File sharing software**
- **Accidentally corrupting or destroying others' data without notifying a member of staff**
- **Accidentally accessing offensive material and not notifying a member of staff to it.**

Possible sanctions = referred to class teacher, Computing lead teacher and Head teacher. Removal of internet access rights for a period / confiscation of phone / contact with parent/guardian.

Level 3 infringements

- **Deliberately corrupting or destroying someone's data, violating privacy of others**
- **Sending an email or message that is regarded as harassment or of a bullying nature**
- **Deliberately trying to access offensive or pornographic material.**

Possible sanctions = referred to class teacher, Computing lead teacher, Head teacher/ removal of internet rights for a period + contact with the pupil's parent/guardian.

If inappropriate web material is accessed:

1. **Ensure appropriate technical support filters the site.**
2. **Inform the Local Authority and follow their advice.**

<u>Level 4 infringements:</u>

- **Continued sending of e-mails or messages regarded as harassment or of a bullying nature after having been warned**
- **Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent**
- **Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act**
- **Bringing the school name in to disrepute.**

Possible sanctions = referred to the Head teacher, contact with parents/guardians, possible school exclusion, refer to Community Police Officer, local authority e-safety Officer.

Other safeguarding actions on level 4:

1. **Secure and preserve any evidence.**
2. **Inform the sender's e-mail service provider if a system, other than the school one, is used. Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school hours – that is, if it is related to school in any way.**

St Nicholas is likely to involve external support agencies as part of any investigation – eg ICT technician support to investigate equipment and data evidence/the Local Authority Human Resources Team.

13. **<u>Rewards</u>**

    Whilst recognising the need for sanctions, it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms; for example, class commendation for good research skills, certificates for being good cyber citizens etc.

14. **Social networking** – pupils are not permitted to use social networking site within school.

15. **E-Safety Education – Pupils. To equip pupils as confident and safe users of ICT, St Nicholas will undertake to provide:**

- ✓ A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
- ✓ Regular auditing, reviewing and revision of the computing curriculum.
- ✓ E-Safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner.
- ✓ Opportunities for pupils to be involved in e-safety education. For example, through peer mentoring, e-safety committee, parent presentations, whole school presentations in assembly.

  To support and develop the above:
- ✓ Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and are guided to validate the accuracy of the information.
- ✓ There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- ✓ St Nicholas actively provides systematic opportunities for pupils to develop the skills of safe and discriminating online behaviour.
- ✓ Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

16. **E-Safety Education – Staff**

- ✓ A planned programme of formal e-safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent Duty.
- ✓ E-safety training is an integral part of Child. Protection/Safeguarding training and vice versa.

- ✓ Staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and also child protection/safeguarding procedures.
- ✓ All new staff receive e-safety training as part of their induction programme, ensuring they fully understand the school e-safety policy and AUP – acceptable Use Policy.
- ✓ Staff are encouraged to undertake additional e-safety training such as CEOP training or with our experience ICT lead/technician.
- ✓ The culture of St Nicholas ensures that staff support each other in sharing knowledge and good practice about e-safety.
- ✓ St Nicholas takes every opportunity to research and understand good practice that is taking place in other schools.
- ✓ Governors are offered the opportunity to undertake training.

17. **Parents and the Wider Community**

There is a planned programme of e-safety sessions for parents, carers etc. This is planned, monitored and reviewed by the DSLs and SLT.

18. **Monitoring and Reporting**

- ✓ St Nicholas's network provides a level of filtering and monitoring that supports safeguarding.
- ✓ The impact of the e-safety policy and practice is monitored through the review/audit of e-safety incident logs, behaviour/bullying logs and surveys of staff, pupils, parents and carers.
- ✓ The records are reviewed/audited and reported to senior leaders and the governing board.

Review statement: this policy is brought to the attention of staff, pupils and parents in the Autumn Term each year; it is formally reviewed every two years. The policy is monitored less formally via staff meetings.

Next review – March 2023

Appendix 1 – AUP

ACCEPTABLE USE POLICY FOR LEARNERS IN KEY STAGE 1

At St Nicholas, I want to feel safe all of the time.

I agree that I will do the following:

- ✓ Always keep my passwords a secret.
- ✓ Only open pages which my teacher has said are ok.
- ✓ Only work with people I know in real life.
- ✓ Tell my teacher if anything makes me feel scared of uncomfortable on the internet.
- ✓ Make sure all messages I send are polite.
- ✓ Show my teacher if I get a nasty message.
- ✓ Not reply to any nasty message or anything which makes me feel uncomfortable.
- ✓ Not give my mobile phone number to anyone who is not a friend in real life.
- ✓ Only email people I know in real life or if my teacher agrees.
- ✓ Only use my school email address in school.
- ✓ Talk to my teacher before using anything on the internet.
- ✓ Not tell people about myself online – I will not tell them my name, anything about my home, family and pets.
- ✓ Not upload photographs of myself without asking a teacher.
- ✓ Never agree to meet a stranger.

- ❖ ANYTHING I DO ON THE COMPUTER MAY BE SEEN BY SOMEONE ELSE.
- ❖ I KNOW HOW TO REPORT ANY PROBLEMS.

Signed	
Name in capital letters	
Class	
Date	

Thank you from all of the staff and governors at St Nicholas C of E Primary School. Our mission is to keep you safe at all times.

ACCEPTABLE USE POLICY FOR LEARNERS IN KEY STAGE 2

At St Nicholas, I want to feel safe all of the time.

I agree that I will do the following:

- ✓ Always keep my passwords a secret.
- ✓ Only use, move and share personal data securely.
- ✓ Only visit sites which are appropriate.
- ✓ Work in collaboration only with people my school has approved and will deny access to others.
- ✓ Respect the school network security.
- ✓ Make sure all messages I send are respectful.
- ✓ Show a responsible adult any content that makes me feel unsafe or uncomfortable.
- ✓ Not reply to any nasty message or anything that makes me feel uncomfortable.
- ✓ Not use my own mobile device in school unless I am given permission.
- ✓ Only give my mobile phone number to friends I know in real life and trust.
- ✓ Only email people I know in real life or those who are approved by St Nicholas School.
- ✓ Only use the email which has been provided by my school.
- ✓ Obtain permission from a teacher before I order online.
- ✓ Discuss and agree on my use of a social networking site with a responsible adult before joining.
- ✓ Always follow the terms and conditions when using a site.
- ✓ Always keep my personal details private – my name, my family information, the journey to school, my pets and hobbies; all personal information will not be shared.
- ✓ Always check with a responsible adult before I share images of myself or others.
- ✓ Only create and share content that it legal.
- ✓ Never meet an online friend in real life as they may not be the person I have communicated with online. Someone who says they are 11 years old online might be much older in real life.
  - ❖ ANYTHING I DO ON THE COMPUTER MAY BE SEEN BY SOMEONE ELSE.
  - ❖ I KNOW HOW TO REPORT ANY PROBLEMS.
  - ❖ I KNOW THAT ONCE I SHARE ANYTHING ONLINE, IT IS COMPLETELY OUT OF MY CONTROL AND MAY BE USED BY OTHERS IN A WAY THAT I DID NOT INTEND.

Signed	
Name in capital letters	
Class	
Date	

Thank you from all of the staff and governors at St Nicholas C of E Primary School. Our mission is to keep you safe at all times.

ACCEPTABLE USE POLICY (AUP) FOR ANY ADULT WORKING WITH LEARNERS AT ST NICHOLAS C of E PRIMARY SCHOOL

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- ✓ only use, move and share personal data securely.
- ✓ respect St Nicholas network security.
- ✓ implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources.
- ✓ respect the copyright and intellectual property rights of others.
- ✓ only use approved email accounts.
- ✓ Only use pupil images or work when approved by parents/guardians and in a way that will not enable individual pupils to be identified on a public-facing site.
- ✓ Only give permission to pupils to communicate online with trusted users.
- ✓ Use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- ✓ Not use or share my personal (home) accounts/data – eg Facebook, email, eBay, Amazon etc. with pupils.
- ✓ Set strong passwords which I will not share and will change regularly – a strong password is one which uses a combination of letters, numbers and other permitted symbols.
- ✓ Report unsuitable content and/or ICT misuse to the ICT subject leader and/or the DSL or DDSL (designated safeguarding officer or their deputy)
- ✓ Promote any supplied E-Safety guidance appropriately.

    - ❖ I KNOW THAT ANYTHING I SHARE ONLINE MAY BE MONITORED.
    - ❖ I KNOW THAT ONCE I SHARE ANYTHING ONLINE THAT IT IS COMPLETELY OUT OF MY CONTROL AND MAY BE USED BY OTHERS IN A WAY THAT I DID NOT INTEND.

I agree that I will not:

- Visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:
  - Inappropriate images
  - Promoting discrimination of any kind
  - Promoting bullying or violence
  - Promoting racial or religious hatred
  - Promoting illegal acts
  - Breach any Local Authority/St Nicholas C of E Primary School's policies. One example would be gambling.
  - Do anything which exposes others to danger.
  - Post any other information which may be offensive to others.
  - Forward chain letters which breach copyright law
  - Use personal digital recording equipment including cameras, phones or other personal devices for taking/transferring images of pupils or staff without their permission.
  - Store images or other files off-site without permission from the Head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any personal information I see regarding staff or pupils which is held within St Nicholas C of E Primary School's management information system (MIS) private, secure and confidential. The only exception to this is when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of St Nicholas C of E Primary School's ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

Name in capital letters _____

Date _____

Thank you for keeping yourself and your school community safe.

AUP (Acceptable Use Policy) Guidance for Schools and Governors
St Nicholas Church of England Primary School

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc) is used to support learning without creating unnecessary risk to users.

We, as governors, will ensure that:

- ✓ learners are encouraged to enjoy the safe use of digital technology to enrich their learning.
- ✓ learners are made aware of risks and processes for safe digital use.
- ✓ all adults and learners have received the appropriate acceptable use policies and any required training.
- ✓ an E-Safety Policy has been written by St Nicholas C of E Primary School.
- ✓ the E-Safety Policy and its implementation will be reviewed regularly.
- ✓ the school internet access is designed for educational use and will include appropriate filtering and monitoring.
- ✓ copyright law in not breached.
- ✓ learners are taught to evaluate digital materials appropriately.
- ✓ parents are aware of the AUP – acceptable use policy.
- ✓ parents will be informed that all technology usage may be subject to monitoring, including URLs and text.
- ✓ St Nicholas will take all reasonable precautions to ensure that users access only appropriate material.
- ✓ St Nicholas will audit the use of technology and will establish if the E-Safety Policy is adequate and appropriately implemented.
- ✓ methods to identify, assess and minimise risks will be reviewed regularly.
- ✓ complaints of internet misuse will be dealt with by senior members of staff at St Nicholas C of E Primary School.

Appendix 2 – Parent Letter – Internet/Email

St Nicholas Church of England Primary School

Parent/Guardian Name	
Pupil Name	
Pupil Class Name	

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the internet, the virtual learning environment, school email and other ICT/computing facilities at school. I know that my son or daughter has signed a form to confirm that they will keep to St Nicholas Church of England Primary School's rules for responsible ICT/computing use, outlined in our AUP – Acceptable Use Policy which can be found on the school's website – safeguarding tab.

I also understand that my son(s) /daughter(s) may be informed if the rules have to be changed during the year.

I accept that ultimately St Nicholas C of E Primary School cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate material. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching E-Safety skills to all pupils.

I understand that the school can check my child's computer files and the internet sites they visit. I also know that the school may contact me if there are concerns about my child's E-Safety or E-Behaviour. I will support the school by promoting safe use of the internet and digital technology at home and I will inform the school if I have concerns over my child's (or any other child's) E-Safety.

I am aware that St Nicholas C of E Primary School permits parents/guardians to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking sites, such as Facebook, if the photos/videos contain images of other children. I will support the school's approach to E-Safety and will not upload or add any pictures, videos or text that could upset, offend or threaten the safety of any member of the St Nicholas Church of England Primary School's Community.

Parent/Guardian Signature	
Parent/Guardian name in CAPITAL LETTERS	
Date	

SCHOOL AUDIT FOR E-SAFETY

St Nicholas Church of England Primary School

The self-audit should be completed by the Head Teacher /DSL in liaison with the Computing Subject Leader.

Date of the latest update:	
The Leadership Team Member responsible for E-Safety at St Nicholas:	
The governor responsible for E-Safety is:	
The designated members of staff for child protection is:	
The E-Safety and Computing Lead is:	
The E-Safety Policy and Acceptable Use Policies were approved by the Governing Board on:	
The policies are available for staff:	School website www.stnicholashenstridge.co.uk and Policy File in the school office and shared staff Google Drive.
The policies are available for parents/guardians:	School website www.stnicholashenstridge.co.uk and Policy File in the school office
Date of E-Safety training for staff:	
Date of Prevent Training:	

A completed hard copy of this page is kept in the school's safeguarding folder.

It is signed off by the Head Teacher & DSL when completed.