Computer Curriculum and ICT Support
10point4education

St John's Primary E-Safety Policy

1.0 Who will write and review the policy?

Senior Manager with responsibility for whole school ICT:	Tracey Caffrey
ICT Subject Leader:	Roberta Branson
Safeguarding Responsibility:	Tracey Caffrey
Technician:	Local authority contract
ICT Governor:	Marie Bartley

Monitoring of the Information and Communication Technology (ICT) policy is the responsibility of the ICT Team and Senior Management of the school.

The policy is reviewed each year by the ICT Team and Senior Leadership Team and fully revised and presented to Governors for final approval every year before being issued to staff.

As Online safety is an important aspect of strategic leadership within the school, the Head teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety Coordinator (OSC) in this school is Tracey Caffrey who has been designated this role as a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the OSC to keep abreast of current issues and guidance through organisations such as Newcastle Local Authority, Department for Education, Child Exploitation and Online Protection Centre (CEOP), and Childnet.

Senior Management and Governors are updated by the Head teacher/OSC and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the school's laptop policy and online rules. It is linked to the following mandatory school policies:

- Child Protection
- Health and Safety
- Home - School Agreements
- Behaviour / Pupil Discipline (including the Anti-Bullying policy)
- PSHE
- Corporate ICT Policies
- Social media policy
- Home learning policy

- Data protection (GDPR)/Privacy notices

2.0 Teaching and Learning

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- Access to world-wide educational resources, including museums and art galleries.
- Inclusion in the National Education Network (www.nen.gov.uk) which connects all UK schools.
- Educational and cultural exchanges between pupils world-wide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and access to learning wherever and whenever convenient.

Our aim is to produce learners who are confident and effective users of ICT. We strive to achieve this by:

- Helping all children to use ICT with purpose and enjoyment.
- Helping all children to develop the necessary skills to fully utilise ICT.
- Helping all children to become autonomous users of ICT.
- Helping all children to evaluate the benefits of ICT and its impact on society.
- Meeting the requirements of the National Curriculum and helping all children to achieve the highest possible standards of achievement.
- Using ICT to develop partnerships beyond the school.
- Celebrating success in the use of ICT.

2.1 Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils are taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet benefits the professional work of staff and is essential to the school's management information and business administration systems.

2.2 Education – Pupils

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and

provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities.
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

2.3 Education – Parents / Carers / Families & the Wider Community

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, websites, Class Dojo
- Parents/guardian sessions
- High profile events / campaigns e.g. Safer Internet Day

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards full families as well as parents/ carers.
- The school website will provide online safety information for the wider community.
- Supporting community groups to enhance their online safety provision.

2.4 Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training is made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The OSC (or other nominated person) will receive regular updates through attendance at external training events.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The OSC (or other nominated person) will provide advice / guidance / training to individuals as required.

2.5 Training – Governors

Governors have taken part in online safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

3 Managing Content and Communication

3.1 How will email be managed?

- Pupils may only use approved email accounts issued by local authority ICT team
- Pupils must immediately tell a teacher if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone
- Whole-class or group email addresses will be used for communication outside of the school
- Access in school to external, personal email accounts will 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
- The forwarding of chain messages is not permitted
- Staff should not use personal email accounts during school hours or for professional purposes

3.2 School website

- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information are not published.
- Email addresses are published carefully, to avoid being harvested for spam. (e.g. you could replace '@' with 'AT'.)
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

3.3 Can pupils images or work be published?

- Images that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers must be obtained before images of pupils are electronically published.
- Pupil's work can only be published with their parent or carer's permission

3.4 How can emerging technologies be managed?

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

3.5 Mobile Devices

This section sets out what is 'acceptable' and 'unacceptable' use of mobile devices by the whole school community (students, staff and visitors) while they are at school or undertaking school activities away from school.

Mobile devices are now a feature of modern society and many of our pupils own one. The technology of mobile devices has developed such that they now have the facility to record sound, take photographs and video images and connect to the internet. Therefore, the school also recognises the advantages mobile devices have as a ubiquitous learning tool.

3.5.1 General issues

- Mobile Technology should only be used in school with the permission of a member of staff and in accordance with their instructions.
- Mobile devices brought into school are entirely at the staff member, student's & parents/carers' or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- The school allows staff to bring in personal mobile phones and devices.
- All visitors are requested to keep their phones on silent.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents/carers or students need to contact each other during the school day, they should do so only through the school office.
- Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used for any aspect

of school business (e.g. contacting parents, taking photographs and videos, tweeting and Facebook status updates).

- Where the school provides mobile technologies such as phones, laptops and tablets for off-site school business, wherever possible these should not be taken home and should be stored in a secure location on school premises.
- Personal use of school owned devices is prohibited unless specifically approved by the head teacher or equivalent, and in accordance with the finance policy of the school.

3.5.2 Students use of mobile devices

- The school strongly advises that student mobile phones and devices should not be brought into school.
- The school accepts that there may be particular circumstances in which a parent/carer wishes their child to have a mobile phone for their own safety but all phones must be handed into the school office at the start of the day and collected at the end of the day.
- Where a pupil is found with a mobile in school, including the playground, the phone will be taken from the pupil and placed in the office. Parents may be contacted to collect the phone
- Pupils should be encouraged to mark their mobile device clearly with a form of identification, and use a tracking service where available. It is strongly advised that students use passwords / pin numbers to ensure that unauthorised calls cannot be made on their devices.
- The school cannot take responsibility for loss or damage to pupils' personal mobile technology. Devices should not be left unattended in school, e.g. in bags or table trays.
- Parents/carers should be aware of the potential risks for children of using mobile technology such as theft, bullying and inappropriate contact, including grooming by unsuitable persons.
- Parents/carers are encouraged to ensure that suitable tracking and filtering systems are activated on mobile technology used by their children.
- If a pupil is found taking photographs or video footage with a mobile phone of either pupils or teachers, this will be regarded as a serious offence and the Head teacher will decide on appropriate disciplinary action. If images of other pupils or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by an appropriate person
- If a pupil needs to contact his/her parents/guardians they will be allowed to use a school phone. If parents need to contact children urgently they should phone the school office and a message will be relayed promptly
- It is the responsibility of parents and pupils to ensure mobile devices are adequately insured.
- If a pupil breaches these rules the phone will be taken from the pupil and placed in the office. Parents may be contacted to collect the phone

3.5.3 Staff use of mobile devices

- Staff should ensure they cannot be distracted from their work with children. For example, phones should be turned off and put away beyond use when not needed.
- It is essential that staff do not put themselves at risk of allegations.

- Images and video of children should never be taken without having secured signed permission from the parent or carer.
- School devices containing personal information, including photographs and video of children, should not be taken off the premises, except with the explicit agreement of SLT in each and every case.
- Any images taken with permission are the property of the school and should only be used in relation to school business.
- Staff devices may be used to take photos or videos for the purposes of Class Dojo or blogs. Devices will only be used to take photos or videos, when appropriate, where parental permission is in place. All photos or videos must be deleted as soon as they have been used for their intended purpose.
- Staff should never contact a pupil or parent / carer using their personal device unless using the class dojo messaging service. If use of a mobile phone is unavoidable then the mobile number must be withheld.
- School owned devices for staff use should be secured with a pin code and should not be left unattended or on display. Any loss or theft of school owned devices should be reported to the Head teacher or equivalent immediately.
- Personal devices may be used for teaching activities, but should have all notifications (for emails etc.) shut off, to avoid personal information being shared and displayed accidentally with pupils.
- Personal mobile devices should NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropbox etc.).
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Where St John's Primary School/setting provides mobile devices for off-site school business, wherever possible these should not be taken home and should be stored in a secure location on school premises
- "Malicious communication" between any members of the school community is not allowed, e.g. text messages or online chat.
- Staff should be mindful that photographs and video taken of colleagues during working hours should not be shared without permission of all those concerned and the Head teacher or equivalent
- If a member of staff breaches the school policy then disciplinary action may be taken.

School ensures that all staff adhere to the "Acceptable Use Policy" – which is signed by staff, pupils and parents via the home school agreement - and that common sense is used at all times.

3.5.4 Class Dojo, Seesaw & Class blogs

Seesaw is a safe and secure system and enables families to access their child's learning journey at any time. They can share it with their child, family and friends at home and also post any comments and photographs of their own, helping to create a fully holistic view of the child and strengthen the parent partnership. Class Dojo is an

online app which allows staff to share information about children's behavior, attitude and learning directly with parents and to develop a two-way conversation about the child. In addition, all classes in school use class blogs to share information with parents on the activities which children have participated in during the school week. This information is available to anyone access the blog via the school website.

- Seesaw and Class Dojo allow staff and parents to access the information from any computer or device via a personal, password-protected login.
- Staff access allows input of new observations and photos or amendment of existing observations and photos.
- Parent access allows input of new observations and photos or the addition of comments on existing observations and photos – parent log-ins do not have the necessary permission to edit existing material.
- Parents logging into the system are only able to see their own child's Learning Journey or Dojo area, but will also be able to view children other than their own in photographs.
- Parents are asked to sign a consent form giving permission for their child's image to appear in other children's Learning Journeys or Dojos, and to protect images of other children that may appear in any photos contained in their child's Learning Journey or Dojo.
- A child's learning journey and Dojo 'story' is a document recording their learning and development and parents may add comments on observations or contribute photos, videos or information about activities they have been doing at home.
- The Seesaw Learning journey system is hosted on secure dedicated servers based in the UK. It has a data security policy in line with GDPR
- Access to information stored on Seesaw and Dojo can only be gained by unique user id and password. Personal data belonging to parents is not accessible via teacher pages.
- Staff use ipads, their own mobile phones or school cameras to take the photographs for observations but these will not be stored on the device. Photos will be uploaded to the journal as they are taken and then deleted at once from the device. Class Dojo only saves photos into the app and no record of the photo appears on the member of staff's own phone.
- The acceptable use agreements are signed by parents and staff and state that they agree to use the systems in accordance with the guidelines.

The governors of St John's have carefully considered the issues surrounding the sharing of information and whether to allow staff to use their own devices to take photographs for Seesaw, Dojo, blogs or for the school's own social media. School leaders are satisfied that the high levels of safeguarding training undertaken by staff ensure they are fully aware of their responsibilities to safeguard children and that the school's Code of Conduct set out clearly the procedures which must be followed.

Those parents without access to the internet are invited into school to view their child's learning journey. We endeavor to provide a device or a method for accessing the internet wherever possible.

3.5.5 Wearable Technology
Staff

If Wearable Tech is worn in lessons or in public areas around the school, the 'Do not disturb'/'flight mode' should be activated.

Pupils

Wearable Technology that has the ability to communicate, ie Camera, Microphone or message notifications, are not allowed to be worn in school. Pupils must seek permission from the school before wearing fitness tracking devices.

If a Wearable Tech device is deemed by the teacher to be causing a distraction around school, it is liable to confiscation until the end of the school day.

3.6 Laptops

- Staff provided with a laptop or ipad purchased by the school can only use it for private purposes at the discretion of the head teacher. Such laptops remain the property of the school and are open to scrutiny by senior management, contracted technicians and the ICT subject leader.
- Laptops belonging to the school must have updated antivirus software installed and be password protected.
- Staff provided with a laptop purchased by the school are responsible for updating the antivirus software by connecting to the school network.
- Staff intending to bring personal laptops on to the school premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop.
- Staff should not attach personal laptops to the school network.
- The security of school laptops is of prime importance due to their portable nature and them being susceptible to theft.

4 Policy Decisions

4.1 Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's computers and ICT equipment.
- All staff must read and sign the 'Acceptable use for staff agreement' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific approved online materials.
- Parents will be informed that pupils will be provided with supervised Internet access via the home school agreement.

4.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material through the use of Smoothwall filtering systems. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never appear on a computer connected to the school network. The school or Newcastle Local Authority does not accept liability for any material accessed, or any consequences resulting from Internet use.
- The final decision when assessing risks will rest with the head teacher.

4.3 Monitoring & Filtering

- All internet use is subject to the Smoothwall monitoring and filtering system. This applies to all PCs, laptops, Chromebooks and Satellite Pros used either in school or

at home for both staff and pupil. Smoothwall monitoring and filtering (M&F) ensures that school is fully compliant with KCSIE Sept 2024.
- Designated Safeguarding leads have full access to all M&F reports. Urgent alerts are received for any incidents which are rated above a category four.
- All incidents are addressed in line with the school's safeguarding policy.

4.4 Handling Online safety complaints

- Complaints of ICT/Internet misuse must be recorded and will be dealt with by a senior member of staff, who will decide if sanctions are to be imposed.
- Any complaint about staff misuse must be referred to the head teacher who will decide if sanctions are to be imposed.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- The head teacher will arrange contact/ discussions with Newcastle Local Authority and the police to establish clear procedures for handling potentially illegal issues.
- Any complaint about illegal misuse must be referred to the head teacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by Newcastle Local Authority.
- All staff, pupils and parents will be informed of the complaints procedure.
- All staff, pupils and parents will be informed of the consequences of misusing the Internet and ICT equipment.

4.4 Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's Anti-Bullying Policy.
- There will be clear procedures in place to support anyone affected by Cyberbullying.
- All incidents of Cyberbullying reported to the school will be recorded.

There are clear procedures in place to investigate incidents or allegations of Cyberbullying:

- Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/Carers may be informed.
- The police will be contacted if a criminal offence is suspected.

5 Disseminating the Policy

5.1 Sharing with pupils

- Online safety rules and posters will be displayed in all rooms where computers are used and highlighted/discussed during ICT sessions.
- Pupils are made aware that the network and Internet use will be monitored.
- An Online safety training programme has been introduced to raise the awareness and importance of safe and responsible Internet use.
- An Online safety module is included in the Computing scheme of work and PSHE curriculum.

5.2 Sharing with staff

- Staff will be consulted when creating and reviewing the Online safety policy.
- Staff training in safe and responsible Internet use, both professionally and personally, will be provided, including use of social networking sites such as Facebook.
- Every member of staff, whether permanent, temporary or supply, will be informed that network and internet traffic will be monitored and can be traced, ensuring individual accountability.

Issue date:	8th January 2018
Reviewed by:	Full governing body
Reviewed annually	February 2024

Appendix I
Online safety Policy Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for the Online safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, Online safety Coordinator and Headteacher.

Does the school have an Online safety Policy?	Y/N
Date of latest update (at least annual):	
The policy was agreed by Governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The responsible member of the Governing Body is:	
The Designated Child Protection Coordinator in school is:	
The Online safety Coordinator is:	
Has Online safety training been provided for all pupils (age appropriate) and all members of staff?	Y/N
Is there a clear procedure for responding to an incident or concern?	Y/N
Do all staff sign a Code of Conduct or Acceptable Use Policy on appointment?	Y/N
Are all pupils aware of the Online safety rules or Acceptable Use Policy?	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 sign and return an agreement that their child will comply with the School Online safety rules?	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
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?	Y/N
Has the school-level filtering been designed to reflect educational objectives and been approved by the SLT?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of the SLT?	Y/N

Appendix II
Legal Requirements

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently.

Appendix III
Further Information and Guidance

BBC
http://www.bbc.co.uk/cbbc/topics/stay-safe

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

Childline
www.childline.org.uk

Childnet
www.childnet.com

Digital Literacy
www.novemberlearning.com

Digizen.org.uk
http://www.digizen.org/

Information Commissioner's Office
www.ico.gov.uk

Internet Watch Foundation
www.iwf.org.uk

Kidsmart
www.kidsmart.org.uk

Newcastle Schools IT Support Team
Help with filtering and network security
Tel: (0191) 277 7282

South West Grid for Learning
http://www.swgfl.org.uk/OnlineSafety

Think U Know website
www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse
www.virtualglobaltaskforce.com

Acknowledgement
We gratefully acknowledge that this guidance is adapted from information provided by Kent, Hertfordshire County Council, South West and London Grid for Learning
Compiled by S. Khan, C. Johnston & J. Hughes