St John's Primary
E-Safety Policy

November 2017

Computer Curriculum and ICT Support
10point4education

[Updated: September 2017]

Table of Contents

1.0 Who will write and review the policy?

Issue date:	8th January 2018
Reviewed by:	Full governing body
Ratified by Full Governors:	30th January 2018
Review date:	Amended June 2018 to comply with GDPR

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:	Razmin Begum

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 three years 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 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 Online safety Coordinator 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 and Online safety Coordinator 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 following mandatory school policies:

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

- 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 exploit 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 enhances 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 on-line 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, it is best practice that 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

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, VLE
- Parents sessions
- High profile events / campaigns e.g. Safer Internet Day

2.4 Education – The Wider Community

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 grandparents and other relatives as well as parents.
- The school website will provide Online safety information for the wider community.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online safety provision.

2.5 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 Online safety Coordinator / Officer (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 Online safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

2.6 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).

3.1 How will email be managed?

- Pupils may only use approved email accounts
- 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's permission, (see Appendix VII).

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.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

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 some 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 his / her instructions.
- Mobile devices brought into school are entirely at the staff member, student's & parents' or visitors 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 children are to hand their phones into the school office at the start of the day and collect them at home time.
- Staff devices may be used to take photos or videos for the purposes of Class Dojo, Tapestry 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.
- All visitors are requested to keep their phones on silent.
- Staff devices may be used to contact a parent using class dojo as no personal contact information is displayed. If an emergency arises and a member of staff must use their device to contact a parent then the personal number must be withheld.
- 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 or students need to contact each other during the school day, they should do so only through the School office.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- 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.

- It is the responsibility of parents and pupils to ensure mobile devices are adequately insured.
- If a pupil breaches these rules or 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

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 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
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- 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 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 are encouraged to ensure that suitable tracking and filtering systems are activated on mobile technology used by their children.

3.5.3 Staff use of mobile devices

This policy sits alongside the Tapestry, Class Dojo and Class Blogs policy at Annex 1, please read both documents as there are some exceptions to the rules on the use of staff phones.

- 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,

a) except where parental permission has agreed to staff using photographs and video for assessment purposes.

Or

b) 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 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.).
- If a member of staff breaches the school policy then disciplinary action may be taken.
- 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.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- "Malicious communication" between any members of the school community is not allowed, e.g. text messages or online chat.

Schools and settings should ensure that staff adhere to their "Acceptable Use Policy" – which should be signed by staff, pupils, governors and parents - and that common sense is used at all times.

3.5.4 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 warn 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 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.
- See School Laptop policy (Appendix IV).

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 asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access (see Appendix II).

4.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material through the use of corporate 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 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.

4.5 Managing the School VLE (the Virtual Learning Environment)

- Senior Leadership Team and staff monitor the usage of the VLE by pupils and staff regularly in all areas, in particular communication tools and publishing facilities.
- Pupils/staff are advised on acceptable conduct and use when using the VLE.
- Only members of the current pupil, parent/carers and staff community have access to the VLE.
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff, pupils etc. leave the school their account and access to specific school areas will be disabled or transferred to their new establishment.

Any concerns with content may 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 VLE for the user may be suspended at the discretion of the SLT.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer may be informed.

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 will be 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.

St John's Primary
Tapestry, Class Dojo and Class Blogs Policy

At St John's Primary we use an online system called Tapestry to record and store all observations and assessments relating to each child in Early Years Foundation Stage. This is a safe and secure system and one that 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.

Procedures

Both Tapestry 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.

Security

The Tapestry on-line Learning journey system is hosted on secure dedicated servers based in the

UK. Tapestry have a data security policy in line with GDPR

Access to information stored on Tapestry 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 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 Tapestry, 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 and E-safety policy set out clearly the procedures which must be followed.

Parents sign an agreement stating that they agree to use tapestry in accordance with the guidelines – see attachment.

Staff also sign an agreement stating that they agree to the guidelines – see attachment.

Parents without internet

Those parents without access to the internet are invited into school to view their child's learning journey. We also offer Tapestry sessions each half term where we can support parents with using Tapestry and uploading their own observations.

Date: November 2016 Review Date: January 2018

TAPESTRY
ONLINE LEARNING JOURNAL

Agreed guidelines for accessing and using Tapestry 'Online Learning Journeys', Class Dojo and the school's social media accounts

As a parent/carer I will…

- **Not** publish any of my child's observations, photographs or videos on any social media site.
- Keep the login details for Dojo and Tapestry within my trusted family.
- Speak to a member of staff if I experience any difficulties accessing my child's learning journey.
- Only add appropriate photos/comments that are linked to my child's learning.

I agree to the guidelines and give permission for St John's Primary School to create an online Tapestry Learning Journey/Class Dojo account for;

…… (Child's full name).
The e-mail address I would like to link with the account so I have access to my child's Learning Journey is;

……
(provide your e-mail address)
OR

If you do not have access to e-mail please tick this box and you will be able to view your child's learning Journey using school equipment during specific times throughout the year. ☐

I give permission for my child to appear in other children's learning journeys;

Yes ☐ No ☐

Signature:_____Date: _____

Tapestry Staff Guidelines

All users of Tapestry, Class Dojo, website and social media updates (including blogs) must adhere to the following guidelines and sign below;

- To regularly update new observation and blog entries
- To relate observations to the child's learning
- Staff will only take appropriate photos linked to children's learning/ characteristics of learning. Please note that photo evidence for Health and Self does **not** include toileting needs or dressing and undressing (other than fastening coats and a button on closed shirts)
- To delete photos held on the devices once they have been uploaded to Tapestry, social media or website
- For staff to log into Tapestry or Dojo using their own password details
- For staff to keep their log in details safe and not share them with anyone
- If staff are taking school Ipads home they must **not** allow anyone else to use it
- Ipads are only to be used for work related purposes
- Images and videos are **not** to be exported onto any home devices

I agree to adhere to all of the above guidelines and will use Tapestry, Dojo, social media and website updates in a professional manner.

Name:……

Sign:…… Date:……

St John's Primary

Acceptable Use Agreement for Staff

ICT and the related technologies such as e-mail, the Internet and mobile devices form part of our daily life within school. To ensure that all adults within the school setting are aware of their responsibilities when using any form of ICT all staff must sign this Acceptable Use Agreement and adhere to its content at all times. This is to ensure staff provide positive role models to pupils for the safe and responsible use of online technologies and also safeguard themselves from any potential allegations or inadvertent misuse.

- I know that I should only use the school equipment in an appropriate manner and for professional use in accordance with the Online safety Policy
- I will not give out personal information (mobile phone number, personal e-mail address etc) to pupils or parents
- I will only use the approved, secure e-mail system (name@schoolname.newcastle.sch.uk) for any school business
- I know that I should complete virus checks on my laptop and other portable devices so that I do not inadvertently transfer viruses onto the school network or other ICT equipment
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will ensure school data is stored securely and used appropriately in accordance with school and other relevant policies
- I will report any accidental misuse of school ICT, or accidental access to inappropriate material, to the ICT Subject Leader or Head teacher
- I will not connect any personal device (laptop, digital camera etc), to the school network without authorisation from the Head teacher
- I will respect copyright and intellectual property laws
- I understand that all my use of the Internet and other related technologies can be monitored and logged and made available to the Head teacher
- I will ensure that my online activity, both in and outside school, will not bring myself or the school into disrepute (this includes postings on social networking sites and apps e.g. Facebook, Twitter, Instagram)

I have read, understood and agree to this code of conduct. I will support the safe and secure use of ICT throughout the school. I am aware I may face

disciplinary action if I fail to adhere to it.

Signature: _____ Date: _____

Print Name: _____

St John's Primary

Code of Conduct for Pupils

I agree to follow these rules when using the Internet:

- I will not share my username, password or personal information with anyone else
- I will make sure that ICT communication with other users is responsible, polite and sensible
- I will not look for, save or send anything that could be upsetting or cause offence. If I accidentally find anything like this I will tell a teacher immediately
- I will only upload materials which are free from copyright and suitable for school use
- I will not deliberately misuse or deface other users' work on the school network or Virtual Learning Environment (VLE)
- I understand that if I intentionally misuse the VLE I will lose my access privileges. Further action may also be taken in line with school and Local Authority Policy
- I know that my use of the Internet is monitored and further action may be taken if a member of school staff is concerned about my safety
- I will be responsible for my behaviour when using the Internet because I know that these rules are designed to keep me safe
- I will keep my phone switched off (not on silent mode) and hand it in to the main office before the start of the school day and collect it at the end of the day
- I understand and agree to the rules above and am aware there may be sanctions if I do not follow them

Signed: _____

Class: _____

Date: _____

St John's Primary

Supporting Letter

Dear Parent / Carer

As part of an enriched curriculum your child will be accessing the Internet; viewing websites, using email and the school Virtual Learning Environment (VLE).

In order to support the school in educating your child about Online safety (safe use of the Internet), please read and discuss the Online safety rules attached with your child then sign and return the slip below.

Should you have any concerns and wish to discuss the matter further please contact Miss Bartley via the school office.

Yours Sincerely

Tracey Caffrey
Headteacher

✂_____

Online safety Acceptable Use Rules Reply Slip

I have read and discussed the rules with _____ (child's name) and confirm that he/ she has understood what the rules mean and agrees to follow the Online safety rules to support the safe use of ICT at St John's Primary School.

Parent/ Carer Signature: _____

Print name: _____

Date: _____

St John's Primary

Laptop Policy for Staff

Staff provided with a laptop purchased by the school, agree to the following terms of use:

1 The laptop remains the property of St John's Primary School and is for the use of the person it is issued to and must be returned to the school if and when the teacher leaves employment at the school.

2 The laptop is open to scrutiny by senior management, contracted technicians and the ICT Subject Leader at school.

3 Acceptable Use – teachers should accept and adhere to the school's Acceptable Use Policy, particularly with regard to Internet access.

4 The loading of additional software must be authorised by the school , support teaching and learning and be compliant with the following regulations:

- **Copyright, Designs and Patents Act 1988**
  Specifies that all software must be used only in accordance with the terms of the licence. Generally, the making of copies is forbidden and is a criminal offence.
- **Computer Misuse Act 1990**
  Identifies three main offences concerning unauthorised access to systems, software or data.

If you are in any doubt please speak to your school or LA before loading any software

5 Anti-Virus software must be installed and should be updated on a regular basis. School ICT staff will advise on the routines and schedule of this operation. Sophos anti-virus updates are available from school and are covered by the Local Authority licence.

6 Staff are responsible for updating and maintaining the antivirus software at home.

7 All repair and maintenance of laptops must be conducted under the terms and conditions of the warranty.

8 Data Protection – the terms of the school's GDPR policy should be adhered to and users must clearly understand that there is a personal legal duty on them as well as the school.

9 Any charges incurred by users accessing the Internet from home are **not** chargeable to the school.

10 Staff should not connect personal laptops onto the school network.

11 Failure to comply with these guidelines and the school's Acceptable Use Policy, may result in the withdrawal of the laptop and may lead to disciplinary proceedings.

Laptop Details:

Make: _____

Model: _____

Serial Number: _____

Authorised by Head teacher:

Signed: _____

Date: _____

Member of Staff:

Print name: _____

Signed: _____

Date: _____

St John's Primary

Mobile Phone Policy

- St John's Primary School discourages pupils from bringing mobile phones to school
- The phone must be clearly labelled with the child's name, switched off and given in to the office on arrival at school
- The phone must be collected at the end of the school day from the office
- The phone must be concealed whilst leaving the school premises
- 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
- 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
- Parents are advised that St John's Primary School accepts no liability for the loss or damage to mobile phones which are brought into the school
- 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

This policy became operational from 8th January 2018
The policy may be amended from time to time in accordance with school development and any changes to legislation.

St John's Primary

Mobile Device Policy

This policy sits alongside the Tapestry, Class Dojo and Class Blogs policy at Annex 1.

- St John's Primary School allows staff to bring in personal mobile phones and devices for their own use during non-contact rest periods only
- Staff devices may be used to take photos or videos for the purposes of Class Dojo, Tapestry 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 devices may be used to contact a parent using class dojo as no personal contact information (of either party) is displayed. If an emergency arises and a member of staff must use their device to contact a parent then the personal number must be withheld.
- School devices will only be used to take photos or videos, when appropriate, where parental permission is in place
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- Where St John's Primary School provides mobile devices 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 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
- 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
- Personal use of school owned devices is prohibited unless specifically approved by the Head teacher.
- St John's PrimarySchool accepts no responsibility whatsoever for theft, loss, damage or health effects, (potential or actual), relating to mobile devices

This policy became operational from 8th January 2018
The policy may be amended from time to time in accordance with school development and any changes to legislation.

Consent form for taking and using photos/ videos

Child's name: «Forname» «Surname»

Date: 8th May 2018

Dear Parent/Carer

At St John's, we sometimes take photographs of pupils. We use these photos in the school's prospectus, on the school's website, on social media and on display boards around school.

We would like your consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school/ Trust to take photographs of my child. ☐

I am happy for photos of my child to be used on the school website. ☐

I am happy for photos of my child to be used in the school/ trust prospectus and other publications such as newsletters ☐

I am happy for photos of my child to be used in internal displays. ☐

I am happy for photos of my child to be used on social media ☐

I am happy for photos of my child to be used in print media such as newspapers and magazines ☐

I am **NOT** happy for the school to take or use photos of my child. ☐

If any other organisation wishes to take photographs or record video then additional consent will be sought.

If you change your mind at any time, you can let us know by emailing marie.bartley@stjohns.newcastle.sch.uk, calling the school on 0191 2735293, or just popping in to the school office.

If you have any other questions, please get in touch.

Why are we asking for your consent again?

You may be aware that there are new data protection rules coming in from May. To ensure we are meeting the new requirements, we need to re-seek your consent to take and use photos and videos of your child. We really value using photos and videos of pupils, to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again.

Parent or carer's signature: _____

Date:

Appendix X

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 XI
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. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation, in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.
The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of

causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment.
This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

General Data Protection Regulations 2018
The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the EU. This updates the Data Protection Act 1998.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files)
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.
The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.
It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious

Hatred Act 2006 it also makes the possession of inflammatory material, with a view of releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"

63 (6) must be "grossly offensive, disgusting or otherwise obscene"

63 (7) this includes images of "threats to a person's life or injury to: anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic"

Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Head Teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

Appendix XII
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