Dinnington First School

E Safety Policy

Newcastle Schools ICT Curriculum Team

[Updated: February 2016]

craig.johnston@newcastle.gov.uk
www.ictcurriculum.xyz

Table of Contents

1.0 Who will write and review the policy?

Issue date:	May 2016
Reviewed by:	A Farrar and Curriculum Committee
Ratified by Full Governors:	27th June 2016
Review date:	June 2018

Senior Manager with responsibility for whole school ICT:	Mrs A Farrar
ICT Subject Leader:	Mr R Donnelly, Mrs E Creed
Safeguarding Responsibility:	Mrs A Farrar
Technician:	Mr A Ethrington
ICT Governor:	Dr C Gamble

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 e-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 e-Safety Coordinator in this school is Mrs A Farrar 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 e-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 e-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)
- PSHCE
- Corporate ICT Policies

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 should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhance the school's management information and business administration systems.

2.2 Education – Pupils

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.
- Pupils should be 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be 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 should 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 should be 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 e-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 e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety.
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-Safety provision.

2.5 Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

2.6 Training – Governors

Governors should take part in e-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 in primary schools for communication outside of the school
- Access in school to external, personal email accounts may / 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 should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

- Email addresses should be 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 should comply 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 most 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 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 for their own use during non-contact rest periods only.
- During contact time personal devices should be switched off and put away beyond use.
- School devices will only be used to take photos or videos, when appropriate, where parental permission is in place.
- All visitors are requested to keep their phones on silent.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal 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 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.

3.5.2 Students use of mobile devices

- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- 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.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- 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

- Staff should ensure they cannot be distracted from their work with children. For example, phones should be turned off and put away beyond use.
- Personal mobile devices should not be used around children, in particular photographs and video should only be taken on school issued devices.
- 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 should never contact a pupil or parent / carer using their personal device.
- 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.
- Staff will be provided handheld devices as the school deems necessary in order to deliver the majority of your role, personal devices should not be used as part of teaching and learning.
- 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.

3.6 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 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 e-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 will be clear procedures in place to investigate incidents or allegations of Cyberbullying:

- Pupils, staff and parents/carers will be 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.

5.1 Sharing with pupils

- e-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 e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use.
- An e-Safety module will be included in the Computing scheme of work and PSHE curriculum.

5.2 Sharing with staff

- Staff will be consulted when creating and reviewing the e-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.