Banister Primary School

E-safety and Information Communication Technology (ICT) Policy

Banister Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults and it applies to all members of the school (including staff, students/pupils, volunteers, contractors, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. This includes the wider use of personal technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

1. Writing and reviewing the E-safety and ICT Policy

The E-Safety Policy and Information Communication Technology (ICT) Policy is part of the School Development Plan and relates to other policies including those for behaviour, anti-bullying and for child protection**.**

The school will appoint an E-Safety co-ordinator. This may be the Designated Child Protection Officer as the roles overlap, but could also be a member of SLT, the ICT co-ordinator or a subject teacher. It is not a technical role.

2. Roles and Responsibilities:

2.1 Governors:

Governors are responsible for the approval of the E-Safety and ICT Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of e-Governor. The role of the e-Governor will include:

- regular meetings with the e-safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to relevant Governors/Board/committee/meeting

2.2 Head Teacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of all members of the school community.

- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

- The Headteacher and Senior Leaders are responsible for ensuring that the e-safety co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

2.3 E-Safety Co-ordinator

The e-safety co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety and ICT policy
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority/outside agencies
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with e-Governor to discuss current issues and review incident logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team
- keeps abreast of local and national e-safety awareness campaigns

2.4 Teaching and Support Staff

Teaching and Support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation/action/ sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the e-safety and acceptable use policies
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these 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

2.5 Child Protection Officer/Safeguarding Designated Person

The designated child protection officer should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal /inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

2.6 Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking /use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s e-safety and ICT policy covers their actions out of school, if related to their membership of the school.

2.7 Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use ICT, including the internet/mobile devices, in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, school website and information about national/local e-safety and ICT campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety and ICT practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

2.8 Community Users, Visitors and Contractors

Community Users, visitors and contractors who access school systems/website as part of the wider school provision will be expected to sign an Acceptable Use Policy (AUP) before being provided with access to school systems.

3. Policy Decisions

3.1 Authorising Internet access

- All staff must read and follow the school Acceptable Use of the Internet policy.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents must sign and return a slip to acknowledge the pupil acceptable use agreement prior to granting access to ICT systems.

3.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Southampton City Council (SCC) can accept liability for any material accessed, or any consequences of Internet use.

The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

3.3 Misuse of school ICT systems or personal technology in school

Banister Primary School takes misuse of school ICT systems, both in and out of the school, including the wider use of personal technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs very seriously. Banister Primary School takes the view that all users of ICT systems do so under the direct code of conduct set out in this policy and under the acceptable use agreements.

3.4 Specific areas of misuse

(Please note: any form of media refers to text, digital image of any type, video and audio file in the rest of this document. This includes the wider use of personal technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs)

- It is an offence under the school's code of conduct for any member of the school community to publish any derogatory remark in any form of media on any of the school's ICT systems or their own personal technology.
- It is an offence under the school's code of conduct for any member of the school community to extract any form of media from the school 's ICT systems or their own personal technology for use in cyber bullying.
- It is an offence under the school's code of conduct for any member of the school community to publish or store any sexist, racist or sexually exploitative material in any form of media on school ICT Systems or their own personal technology.

- It is an offence under the school's code of conduct for any member of the school community to knowingly store or seek to spread a virus using the school's ICT systems or their own personal technology.
- It is an offence under the school's code of conduct for any member of the school community to run a business using the school's ICT systems.

3.5 Dealing with misuse

- To deal with any incidents of cyber bullying that occur as if the bullying had taken place within the physical bounds of the school.
- Following best practise where cyber bullying threatens violence or is of a sexual nature the police will be asked for their advice/involvement.
- Offences will be dealt with according to the level of the offence in line with school discipline for pupils and guidelines for staff disciplinary procedures. If the offence is a breach of criminal law, the police will be called in and all evidence will be preserved to the best of the school's ability. If the offence is committed by a person not employed by Banister, the head teacher will decide how to deal with the offence according to best practice.
- Pupil minor infringements of these rules can be dealt with by a withdrawal of certain ICT privileges (eg. the withdrawal of ability to message other pupils for a fixed period of time - often two weeks for a minor first offence. Pupil would still be able to message teachers).
- As a general principle, pupils would not be withdrawn from virtual learning work areas unless there were extremely good reasons to do so that were in the best interests of the child.
- If a pupil is temporarily excluded from the school, their virtual learning access would not be removed unless it was in their best interest or in the best interests of other pupils within the school.

3.6 Handling e-safety and ICT complaints

- Complaints of ICT and/or internet misuse, will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher, unless it is the Head teacher where complaints will be sent to the Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

4. Introducing the policy

4.1 Introducing the e-safety and ICT policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- E-Safety training will be introduced to the whole school community to raise awareness and importance of safe and responsible internet use.
- E-Safety training will be embedded within the computing programme of study and include both school and home use.

4.2 Staff and the e-safety and ICT policy

- All staff will be given the school e-safety and ICT Policy and its importance explained.
- E-safety training will be made available to all staff.
- All new staff should receive e-safety training as part of their induction, ensuring that they fully understand the school e-safety and ICT policy and Acceptable Use Agreements.
- Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff that manage the filtering systems or monitor ICT use will be supervised by a member of the senior leadership team and have clear procedures for reporting issues.
- The e-safety and ICT policy and its updates will be presented to and discussed by staff in staff meetings and/or INSET days.
- The e-safety co-ordinator will provide advice/guidance/training to individuals as required.

4.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school E-safety and ICT Policy in newsletters and via the school website.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign for the pupil acceptable use agreement when they register their child with the school.
- The school will provide parents/carers workshops on e-safety.
- The school will provide e-safety information for the wider school community.

4.4 Governors and the e-safety and ICT policy

- All governors will be given the school e-safety and ICT Policy and its importance explained.
- E-safety training will be made available to all governors alongside staff training.
- All new governors should receive e-safety training, ensuring that they fully understand the school e-safety and ICT policy and Acceptable Use Agreement.
- All governors will be asked to sign an acceptable use agreement.

5. Electronic communications

5.1 What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones and personal digital assistants (PDA's)
- Internet communications: e-mail and IM
- Webcams and video conferencing
- Wireless games consoles

6. Teaching and learning

6.1 Why the Internet and digital communications are important

The Internet and other digital communications is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.   Pupils use the internet widely outside of school and will need to learn how to evaluate Internet information and to take care of their own safety and security. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

6.2 Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for internet use
- Internet access will be planned to enrich and extend learning activities.   Access levels will be reviewed to reflect the curriculum requirements and age of pupils
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.

6.3 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. informing teacher

6.4 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Whole school and groups emails should be used where appropriate under the guidance of the class teacher.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

6.5 Published content and the school web site

The contact details on the website should be the school address, email and telephone number. Staff or pupils personal information should not be published. E-mail addresses should be published carefully to avoid spam harvesting. The Head Teacher will take overall editorial responsibility to ensure that content is accurate and appropriate. The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

6.6 Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.

- Consider using group photographs rather than full-face photos of individual children.
- Pupils 'full names' will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil image file names will not refer to the pupil by name.
- Use of 'Marvellous Me' is used solely to promote children's work and learning within the school and any photos are sent over a secure network (see http://marvellousme.com/privacy-policy/).

6.7 Social networking and personal publishing

- The school will block/filter access to social networking sites
- Newsgroups will be blocked unless a specific use is approved.
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection)
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils should be advised not to place personal photos on any social network space
- Teachers must be advised not to run social network site spaces for students on a personal basis.

6.8 Managing filtering

The school will work with Southampton City Council to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Co-ordinator.

6.9 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

7. Information Communication Technology (ICT)

7.1 Aims:

- To be aware of technology and its application in everyday life and the wider world.
- To be aware of e-safety both within and outside of the school environment.
- To use Information and Communication Technology (ICT) as a tool for teachers.
- To encourage children to become increasingly independent in their selection and use of Information Communication Technology (ICT)
- To encourage confidence and a positive attitude when using ICT.
- To teach the skills necessary to access ICT and be safe when using the internet.
- To provide regular opportunities to experience various ICT as an integral part of the whole curriculum.

7.2 Approaches:

- By providing a variety of equipment within school and by observation of technology used in everyday life.
- By using software packages, internet and other ICT equipment for a chosen and identifiable purpose.
- By giving support and extending pupils in each area of the computing curriculum.
- By demonstration and providing opportunities to practice skills and procedures.
- By encouraging the use of ICT capability across the curriculum in class, group, paired or individual tasks.

7.3 Computing in the curriculum:

The requirements of the programme of study for the 2014 Computing Curriculum will be met through the school's topic based approach in each year group. As part of the computing curriculum, a programme of e-safety education will be put in place for the whole school community. ICT will continue to be used across the curriculum so that subject skills can be practiced in other areas of the curriculum.

7.4 Early Years and Tapestry:

In the Early years provision for the use of ICT is highlighted in the Early Learning Goals. Children begin to learn basic ICT skills through a variety of activities and experiencing a range of equipment. We provide all children attending an 'online learning journal'. Through the platform of 'Tapestry', which records observations, photos and videos and also provides an opportunity for parents to comment and add their own observations to their own child's journal. This helps to provide a strong partnership between the setting and home as the children develop.

At Banister Primary School we use the secure online system Tapestry which allows staff and parents to access the information via a personal password protected login. Each child is allocated a class teacher who is responsible for their development and the compilation of their learning journals, however all staff are able to capture observations for each others children.

Parents logging into the system are only able to see their child(ren)'s learning journal. Parent access allows them to comment (or 'reply') to observations that staff have inputted as well as adding their own observations and photos/videos. Before parents are linked to their child(ren)'s learning journal they are asked to give permission for their child's photo to appear in other children's learning journals. Before beginning to access the system, parents have to sign to agree not to download and share any information on any other online platforms or social networking sites (such as Facebook). Whilst Tapestry provides a fantastic tool for sharing information between Banister Primary School and parents, is not used as a way of sharing important information. Each child's learning journal is a document to record their learning and development which parents can add comments on or contribute to with information of what they have been doing at home. Any further discussion of progress or concerns will be done during a face to face conversation at the setting during a prior agreed time. Observations are regularly monitored by the managing staff and assessed during staff meetings to ensure they are providing relevant and informative information.

Safe Use Agreement:

- Staff should not share log in or password details with any person.
- Staff should not share any information or photographs relating to children with any person not employed by Banister Primary School.
- Staff should take all responsible steps to ensure the safe keeping of any portable device e.g. iPad that they are using and report any missing devices.
- If accessing Tapestry with a private computer, not on Banister Primary School premises, staff must maintain confidentiality and professionalism.
- All entries on Tapestry must be appropriate.
- All entries on Tapestry remain the property of Banister Primary School.
- At all times staff must comply with Child Protection policies and ICT safe use policies.

7.5 Equal Opportunities:

There will be equal access, as appropriate, for all children to the ICT equipment and materials available. We will endeavor to provide materials that reflect our multicultural society. We are aware of the necessity to provide equipment and materials for children of differing levels of ability and need.

7.6 Assessment and Recording:

- Planning opportunities for equal access to equipment as appropriate.
- A comment on the child’s achievement in Computing will be included in the annual report to parents.
- Levels of skills attainment will be monitored by the ICT co-ordinator.
- Staff will not store confidential files on the hard drives of the curriculum machines.

7.7 Safety and Care:

- All mains (electrical) equipment is checked regularly.
- All staff know and carry out the correct procedures when using equipment.
- Children will be taught correct procedures, as appropriate, when using equipment.
- Equipment will be sited and used with regard to safety.
- Children will be taught about e-safety as part of the computing curriculum.

7.8 Resources:

All classes have access to tablet computers within the classroom and around the school for flexibility. There are also interactive whiteboards and wireless internet access in all classrooms. There is central access to roamers, pixies, calculators, scanners and digital cameras, although all tablets have a camera and video function inbuilt. There is a suitable range of software installed on the tablets which relates to the curriculum.

8. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

This E-Safety and ICT Policy was approved by the Governors on

Appendices:

1. Staff, Governor and Visitor Acceptable Use Agreement/Code of Conduct
2. Pupil Acceptable Use Agreement/E-Safety Rules
3. Parent Letter

4. Banister Primary School e-safety Incident Log

Appendix 1

Staff, Governor, Contractors and Visitor
Acceptable Use Agreement/Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all adults working in school are aware of their professional responsibilities when using any form of ICT. All adults working in school, including staff, governors, visitors and contractors, are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Sarah Lovelock ICT co-ordinator, Jay Cook DSL for E-safety and teaching and learning coach or Kate Vincent, Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and adults are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of school business manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or adults will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, including the wider use of personal technology, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and ICT policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…………………..………… Date ……………………
Full Name ………………………………...(printed)

Job title ………………………………………………………………

Appendix 2

Pupil Acceptable Use Agreement/E-Safety Rules

- I will only use ICT in school to help me learn.
- I will not tell my friends my ICT log-on names or passwords.
- I will only use my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible, including using appropriate language at all times when using e-mail and other online resources.
- I will respect other people's views and beliefs.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher or parents immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behavior when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that any cyber-bullying will be dealt with in accordance with the schools anti-bullying policy.
- I know that my use of ICT will be checked and that if I go against any part of this acceptable use agreement my parent/carer will be contacted if a member of school staff is concerned about my e-Safety. I also understand that I could lose some of my ICT privileges for a period of time.
- I will not bring my personal technology devices into school unless I have explicit prior consent of a teacher.

Appendix 3

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss the e-Safety rules attached with your child and return the slip at the bottom of this page. If you have any concerns or would like further explanation please contact Jay Cook, DSL for E-safety.

Yours

- -✂- -

Parent/Carer signature

We have discussed the e-safety rules and ……………………………………………(child name) agrees to follow them and to support the safe use of ICT at Banister Primary School.

Parent/ Carer Signature …………………………………………………….

Class ………………………………… Date ………………………………

Appendix 4

Banister Primary School e-Safety Incident Log

Details of ALL e-Safety incidents to be recorded by the e-Safety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. All incidents involving Cyber bullying will also need to be recorded on the school's central CPOMs system.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons