E-safety Policy

Created by Miss N. Jobson
July 2014

Introduction

Computer skills are vital to access life-long learning and employment; indeed we must consider these a life-skill. In delivering the Computing curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and email. Such technology presents risks as well as benefits. As Internet use for home, social and leisure activities is expanding it brings young people into contact with a wide variety of influences, some of which could be unsuitable. It is important that schools, as well as parents, adopt strategies for the responsible and safe use of the Internet.

Aims/ Objectives

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Writing and reviewing the e-Safety policy

Biddick Primary and Nursery School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. Our E-Safety Policy has been written by the school, building on LEA and government guidance. It has been agreed by the School Leadership Team and approved by governors. It will be reviewed annually unless Government or LA changes necessitate an earlier review, or a request has come from the Governors or Headteacher.

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 should be recognised that E-Safety is a whole school issue relating to Safeguarding and not specifically an issue of ICT, therefore this policy is linked to other school policies including those for Behaviour, Safeguarding, PSHE and Anti-bullying.

- The school's Senior Information Risk Owner (SIRO) is Mrs Wendy Fowler, Head teacher
- The school's e-safety coordinator is Miss Nicola Jobson
- The school's e-Safety Governor is Mr Wayne Kennedy
- The network is managed by EDIT

Roles and Responsibilities

<u>Governors:</u>
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the e-Safety Governor will include:

- Regular meetings with the e-Safety Co-ordinator / Safeguarding Officer.
- Regular monitoring of e-safety incident logs.
- Reporting to relevant Governors committee / meeting.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders 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.
- The Headteacher and Deputy Head 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 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 policy / documents.
- 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.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with e-Safety Governor to discuss current issues, review incident logs.
- Provides regular and updated e-safety information to parents through the school website, published documents, assemblies, work-shops etc.
- Attends relevant meetings.

Network manager/technician:

- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy.
- To secure the security of the school's ICT systems, ensuring that provision is in place for detection of system misuse or malicious attack (e.g. keeping virus protection up to date)
- To ensure that access controls/encryption exist to protect personal and sensitive information held on school owned devices.
- To ensure effective web filtering is in place and updated on a regular basis.
- To ensure that appropriate back-up procedures are in place so that critical information and systems can be recovered in the event of a disaster.

Staff and the e-Safety policy

- All staff will be given the school e-Safety policy and its application & importance explained.
- To protect all staff and pupils, the school will implement Acceptable Use Agreements.
- All members of staff will be made aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

- The school will highlight useful online tools, which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils (see BPNS E-safety Curriculum Overview).
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school and also to be aware of their responsibilities, therefore:

- Parents/carers are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy through parental surveys and commentary on the school website.
- Parents/carers are asked to read through and sign Acceptable Use Agreements with their child on admission to the school and before entering Key Stage 2.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).

The school regularly supplies information to parents relating to e-Safety in the form of:

- Website postings- there is a separate e-safety page with links to sites like Thinkuknow, Childline, CEOP and other e-safety published materials
- Class newsletter ‘SMART’ articles
- Information assemblies and celebration evenings
- Relevant posters, leaflets and letters

Internet Access

Equipment with Internet access

Equipment in school with internet access includes the ipads, pupil and staff laptops. All of this equipment is connected through the LEA and websites are monitored and blocked as necessary. When pupils are using any of the above equipment they are under adult supervision and reminded of acceptable use. In addition:

- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- All pupils, staff, governors and visitors must read and sign the 'Acceptable Use Agreement' before using any school ICT resource.
- The school will maintain a current record of all those who are granted Internet access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed regularly by the e-Safety Co-ordinator and e-Safety Governor.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy as part of our Computing curriculum.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Emerging technologies

Emerging technologies will be examined for education benefit and a safety check will be carried out before use in school is allowed. Should staff become aware of emerging technologies they should inform the Head teacher or Computing Co-ordinator so that they can be reviewed.

Communicating with others

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety. At BPNS:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils are taught to immediately tell a teacher if they receive offensive e-mail.
- Pupils will be advised not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses are used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations are written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social networking

Social networking Internet sites (such as, MySpace or Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact. At BPNS:

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Delivering e-safety to pupils

Curriculum

E-Safety is embedded within our whole curriculum. We aim to ensure that:

- Pupils are educated on the dangers of technologies that may be encountered outside school –this will be done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are made aware of the impact of cyber bullying and know how to seek help if these issues affect them. Pupils are also made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- 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, guiding the pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be encouraged to use the 'Hector Protector' button to hide any material that they know is unsuitable for viewing. This will instantly cover the whole screen until it can be dealt with by the class teacher.

Promoting the School e-Safety Message

We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis, therefore:

- The e-Safety policy will be re-introduced to the pupils at the start of each school year, e-safety lessons taught each term as part of our Computing Curriculum and through other subjects, such as PSHE, where appropriate.
- 'SMART' posters will be prominently displayed in all ICT areas.
- Positive e-safety achievements are rewarded through the school newsletter, celebration assemblies reward certificates and SMART stickers.
- BPNS regularly participates in annual e-safety events such as Anti-Bullying Week and Safer Internet Day.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites and online gaming, and offer appropriate advice.

Reporting and dealing with incidents and infringements

Incident Reporting

Any security breaches or attempts, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher or e-Safety Co-ordinator.

All staff are made aware of reporting procedures on their induction (see 'Responding to Online Safety Incidents Flowchart').

- Accidental access to inappropriate materials must be immediately reported to the e-Safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LEA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Users are made aware of sanctions relating to the misuse or misconduct by the Headteacher and in their agreed AUA/Code of Conduct.

e-Safety Incident Log

All incidents of concern regarding e-safety are recorded on the form below and kept in the school's e-safety log. This is held in the Head teacher's office along with other safeguarding documentation.

Biddick Primary & Nursery School
eSafety Incident Log

Details of ALL e-Safety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

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

Security

Passwords

Adult users are provided with an individual network, email login username and password, which they are encouraged to change periodically. Staff should only use their email address for work related purposes and not personal matters.

Pupils are provided with class logins and are taught about keeping these safe as part of our Computing curriculum.

Protecting Personal, Sensitive, Confidential and Classified

All personal data at Biddick Primary and Nursery School is recorded, processed, transferred and made available according to the Data Protection Act 1998. All staff are advised to:

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Safe Use of Images

Before photographs of pupils are taken, stored or published, written permission from parents or carers is obtained in line with the school's Photography Policy. This is done through a consent form that all new starters complete at the beginning of their school life at Biddick Primary and Nursery, then each year each pupil remains in attendance. Parents/Carers are made aware that should circumstances change they must inform school immediately so that photographs can be removed and the database can be altered. Pupils' full names will not be connected to these images anywhere on the website/VLE/newspaper.

All staff, governors and visitors are advised that:

- The use, specifically of mobile camera phones, during school time is not acceptable.
- All images must be taken using school equipment and stored on the school server.
- Photographs must be destroyed or deleted from databases once they are no longer required for the purpose for which they were taken.

Images taken by children are subject to the same restrictions as those taken by staff and must be stored accordingly.

Webcams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. conferencing with other schools.
- Misuse of the webcam by any member of the school community will result in sanctions in line with our Behavior Policy.
- Consent is sought from parents/carers and staff, in the same way as for all images.

Video Conferencing

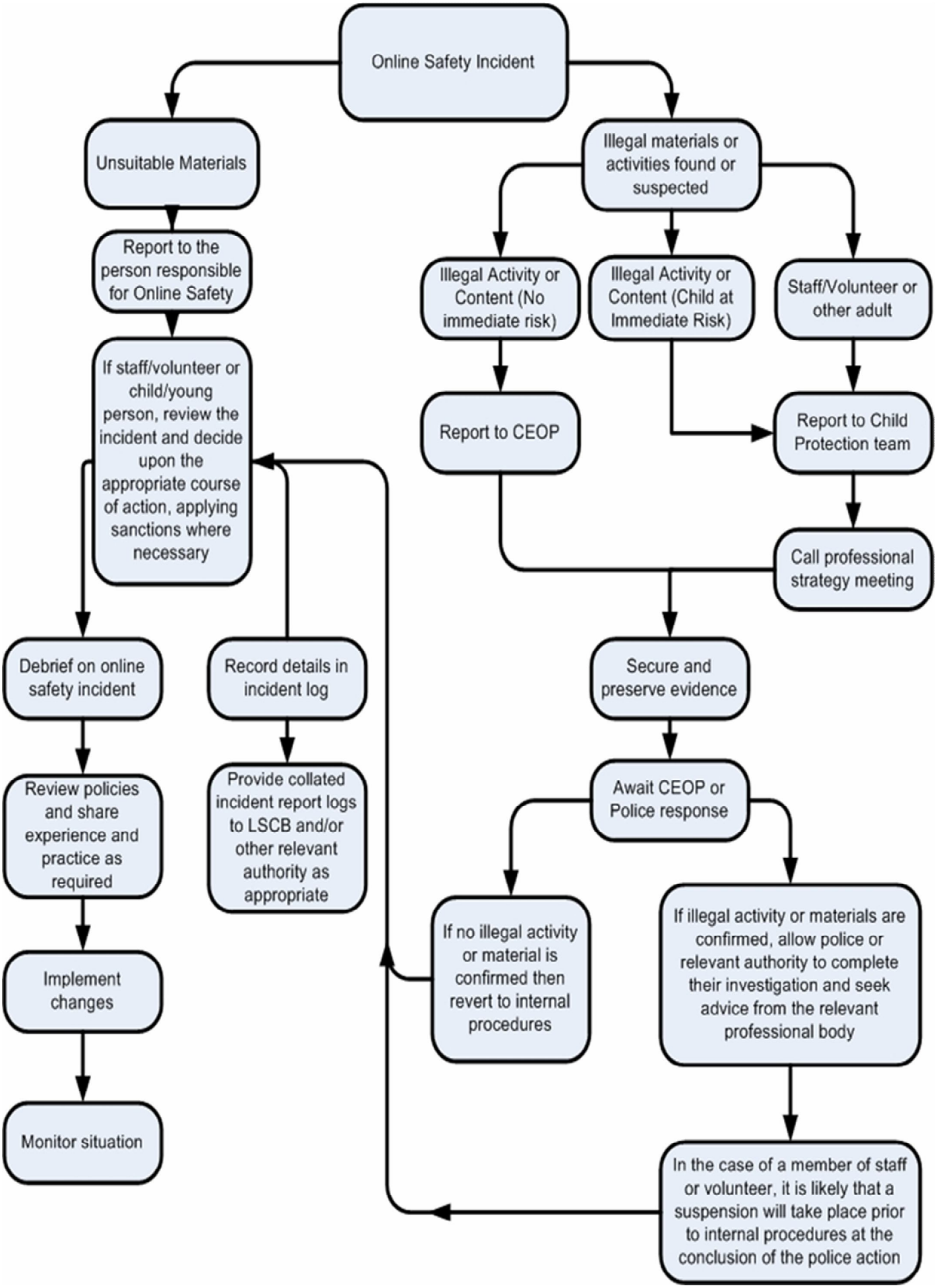
- Permission is sought from parents/carers if their children are involved in video conferences.
- All pupils will be supervised by a member of staff when video conferencing.
- Approval from the Head teacher is sought prior to all video conferences within school.
- School conferencing equipment will not be set to auto-answer, only switched on for scheduled and approved conferences.

Conclusion

This policy needs to be in line with other school policies and should be read in conjunction with:
Computing Policy
Safeguarding Policy
Anti-bullying Policy
Photography Policy

Member of staff responsible: Nicola Jobson
Date policy written: 07/14
Date approved by the Governing body: 09/14
Date to be reviewed: 07/15*

Flowchart for responding to online safety incidents



Be smart on the internet

Childnet International
www.childnet.com

S SAFE

Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE

Information you find on the internet may not be true, or someone online may be lying about who they are.

T TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Foundation/Key Stage One
Acceptable Use of ICT

I want to feel safe all the time, so I agree that I will:

- keep my passwords a secret
- ask an adult before using the internet
- only open pages which my teacher has said are OK
- tell my teacher if anything makes me feel scared or uncomfortable
- only email people I know or if my teacher agrees
- make sure all messages I send are polite
- not reply to any nasty message or anything which makes me feel uncomfortable
- show my teacher if I get a nasty message
- not tell people about myself online. I will not tell them my name, anything about my home and family and pets
- not load photographs of myself onto the computer
- never agree to meet a stranger

I understand that if I break these rules then:

- I could put myself or others in danger
- my parents will be told
- I may not be allowed to use the school's computers or ipads

I have read and understand this policy and agree to follow it.

Pupil:_____

Date:_____

with my child and give permission for him / her to use the school's ICT systems, including the internet.

Parent/Carer: _____

Date:_____

I have read and discussed this policy

Key Stage Two
Acceptable Use of ICT

I want to feel safe all the time, so I agree that I will:

- only use ICT in school for learning purposes and on tasks that my teacher has set
- keep my passwords private
- only use the Internet if a teacher or teaching assistant is in the room with me
- not download or copy and paste content which is copyright
- always use sites and games meant for young people my age
- respect the school ICT equipment and never deliberately alter the settings, install or uninstall any programmes
- only open/delete my own files
- use my class email address or school email address when emailing
- only open email attachments from people I know, or who my teacher has approved
- make sure that all my texts, emails and online conversations are responsible, polite and sensible
- never 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 immediately
- not post online information, photos or videos that could put me at risk or embarrass me or others now or in the future
- never give out personal information such as my name, phone number, school or home address
- only ever meet someone I talk to online if my parent/carer or teacher says it is OK and a responsible adult comes with me
- remember that my use of ICT is monitored and that my parent / carer will be contacted if a member of school staff is concerned about my e-safety
- be responsible for my behaviour when using ICT because I know that these rules are to keep me safe

I understand that if I break these rules then:

- I could put myself or others in danger
- my parents/carers will be informed that I have breached the school's Behaviour and/or Anti-bullying policy
- there will be a consequence such as a ban, temporary or permanent, on my use of ICT at school

I have read and understand this policy and agree to follow it.

Pupil:_____

Date:_____

I have read and discussed this policy with my child and give permission for him / her to use the school's ICT systems, including the internet.

Parent/Carer: _____

Date:_____

Be smart and Think before you Click

Staff, Governor and visitor
Acceptable Use Agreement/Code of Conduct

I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's management information system, will be kept private and confidential, **EXCEPT** when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

I will:

- only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head Teacher or Governing Body.
- use the approved, secure e-mail system for any school business.
- ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- comply with copyright and intellectual property rights.
- ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- only take, store and use images for purposes in line with school policy. Images will not be distributed outside the school network/learning platform without the consent of the parent/carer, and the permission of the Head teacher.
- report any incidents of concern regarding staff use of technology and/or children's safety to the Senior Designated Professional or Head teacher in line with the school's Safeguarding Policy.

- embed the school's e-Safety curriculum into my teaching and help pupils to be safe and responsible in their use of ICT and related technologies.

I will not:

- share or reveal my password(s) to anyone.
- browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
- connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software,
- install any hardware of software without permission of the Headteacher.
- use a mobile phone for any purpose, such as taking photographs or accessing the internet, whilst with individual or groups of children.

User Signature *I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school. I understand that failure to comply with this agreement could lead to disciplinary action.*

Full Name ……(printed)

Signature …… Date ……

BPNS E-safety Curriculum Overview:

Year	Unit + age appropriate resources	Overview
Rec	Unit 1: The Adventures of Smartie the Penguin	Children will learn about who they can trust to ask for help when something is wrong. They will learn that they should never talk to strangers. They will also learn the 'Smartie' e-safety song.
Year 1	Unit 2: Digiduck's Big Decision Hector's World	Children will learn about making suitable choices. Children will understand about asking permission from a friend before using their photograph. They are introduced to Hector the Dolphin and shown how to activate the Hector Protector Button on school devices.
Year 2	Unit 3: Clicky, Router and The Webville Outlaws	Children will learn how to keep safe when using the Internet and who they can trust, if something is wrong. They will also learn the song – 'It's ok to tell'.
Year 3	Unit 4: The Adventures of Kara, Winston and the SMART crew Beat Bullying- Cyber Mentors	Children will be introduced to the SMART crew and will further develop their understanding of the SMART acronym. They will produce materials to promote the SMART rules to other children.
Year 4	Unit 5: The Adventures of Kara, Winston and the SMART crew Netsmartz Kids	Children will be able to understand what information should be kept safe ('information wise'). They will be able to understand who to go to if they are upset and need to tell. They should also understand safety issues about meeting up with people. They will produce raps to be shared in assembly and on the school website.
Year 5	Unit 6: Tracey Beaker – You choose Preventing Plagiarism- Digizen http://zapatopi.net/treeoctopus http://www.allaboutexplorers.com/ http://www.thedogisland.com/ http://www.brookview.karoo.net/Stick_Insects/ http://uncyclopedia.wikia.com/wiki/Is_the_moon_made_of_cheese%3F	Children will learn how to keep themselves safe when talking to friends online, cyber-bullying and plagiarism (including copyright laws). They will be able to understand what a reliable source of information is. They should also understand what is acceptable in terms of reliability of sources.
Year 6	Unit 7: How SMART are you? quiz- Know it all Caught in the Web (Newsround Special) Social Network detective- Digizen Let's fight it together- Digizen	Children will assess how SMART they are. They will learn about social networks and the dangers of sharing information and meeting up with people who they do not know. They will begin to understand how cyberbullying can impact on others and how incidents of cyberbullying can be reported and acted on (including legal ramifications)