NINE ACRES COMMUNITY PRIMARY SCHOOL

South View, Newport, Isle of Wight, PO30 1QP
www.nineacrespri.iow.sch.uk 01983 522984
Headteacher: Mrs E. Dyer BA Hons QTS, NPQH

Team Work Respect Aspiration Perseverance Caring Creativity Citizenship Courage Independence

'Striving for Excellence'

E-Safety Policy

Nine Acres Community Primary School

Approved By:	MIKE SIZER-GREEN
Approval Date:	10 JULY 2017
Review Frequency:	YEARLY
Next Review Due:	9 JULY 2018

SCHOOL GAMES BRONZE

sustrans JOIN THE MOVEMENT

BRITISH COUNCIL INTERNATIONAL SCHOOL AWARD

change 4 Life Eat well Move more Live longer

Introduction to E-Safety

Digital technologies, including the internet, open up learning to children and their ability to explore and interact with the world. However, they can face many dangers using these technologies such as:

- Harmful, illegal or inappropriate content
- Inappropriate communication with strangers or e-bullying
- Risk of being targeted for grooming by those they make contact with
- Loss of personal information
- Inability to evaluate quality, relevance or bias
- Excessive use affecting other development.

It is impossible to eliminate all risks completely so it is essential that we all teach children to understand the potential risks (in an age-appropriate manner that doesn't frighten them) and give them skills to manage the digital world with confidence.

In order to create a safe ICT learning environment, this policy produces detail how the school has:

- an infrastructure of whole-school awareness, designated responsibilities, policies and procedures
- an effective range of technological tools
- a comprehensive internet safety education programme for the whole school community.

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

The school's e-Safety policy will operate in conjunction with other policies including those for Behaviour including Anti-Bullying, Safeguarding and Child Protection.

Our e-Safety Policy has been written by the school, building on County and Government guidance. It has been agreed by the staff and approved by governors.

The e-Safety Policy will be reviewed annually.

Context and Background

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access
- Online gaming; collaboration and in-game communication
- Our whole school approach to the safe use of ICT.

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools, including internet filtering
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching embedded into the school curriculum, schemes of work and wider activities.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Nine Acres Primary School and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school.

Leadership

The Headteacher ensures that the Policy is implemented across the school and takes ultimate responsibility for internet safety issues within school. They will also ensure an appropriate internet safety culture is created in school and that the governing body is informed of any issues.

E-Safety Co-ordinator

Our school E-Safety Co-ordinator is Dave Richardson (IT Manager) alongside Sian Broome (Deputy Headteacher).

The Deputy Headteacher is responsible for keeping up to date on all e-Safety issues and ensuring that staff are updated and receive appropriate training as necessary. As DSL and behaviour-lead, they will take the lead role in exploring suspected cyber-bullying as well as any safeguarding implications.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed.

Staff are required to sign the Acceptable Internet Use agreement annually (See Appendix B).

Class teachers should ensure that pupils are aware of the e-Safety rules, introducing them at the beginning of each new school year and as points of teaching as they arise, in both computer science learning and when ICT is used as a tool across the curriculum.

Children

Children are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school. They also have a responsibility to report any incidents of misuse within school and to seek help from a trusted adult if they experience content or problems online which makes them feel uncomfortable.

Parents

Parents are given information about the school's e-Safety policy and procedures via the school website where recommended self-help websites are listed and recommended. They are also given copies of the children's guidelines and asked to discuss, explore and support these rules with their children.

Technical and Hardware Guidance

Use of the Internet

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 administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access

Our school uses a dedicated and uncontended Lease Line from BT, giving us a fast and direct connection to the internet.

We use a managed and integrated Sophos Web Filtering Appliance. It is located between the school's network and the school's Firewall. This monitors and restricts content as it transfers data between the school and the internet. These filtering rules are updated in real-time to other devices so that the same protection is enforced on the workstations as an additional layer. This helps reduce load on the web appliance from dealing with all internet requests.

Our Firewall is located between the Web Appliance and the Internet connection. It monitors with its own web-filter as a third and final layer, and comes equipped with technology to strip out advertisements and third-party components - allowing for a clean uncluttered web browsing experience.

Modifications in filtering can be submitted by the End-User, to which the IT Manager can reject, accept as well as confirm practicality and usability of any blocks with the End-user prior to any decision being implemented.

Sites are categorised, along with a risk level to user. These categories are then permitted as Site-Wide, Key-Stage, Year Group, Staff or individual, allowing for restrictive use.

Reports can be generated on blocks, usage and frequency for an individual or group of people, automatically or on demand as required.

Any rules that have been marked as "Notify", such as profanity, extremism or suicide are immediately emailed to key staff for action. In most cases, the IT manager attends the classroom with search details, for the leading teacher to action, and where relevant, SLT and Welfare staff.

Not all pages are unblocked on request, if there is doubt or concern, a formal request is made in writing, which is then deliberated over with the Senior Leadership Team for resolution.

We use a Sophos Hosted Anti-Virus platform which means our system is protected in real-time for Viruses, Malware and Ransomware even if the computers are taken off-site; any infections are dealt with automatically, and if not possible, quarantined for action by the IT Manager.

Emails to/from pupil accounts to/from external destinations require them to be moderated first to ensure content and destination is appropriate; this is processed by the IT Manager and where necessary discussed with the lead teacher of that pupil.

However, no system is perfect and children would be encouraged to share any content which causes them concern (see Child responsibilities). Children are not permitted to use the internet without teacher's knowledge and permission.

An integral part of teaching children to become considered, reflective users of the internet is exploration and discussion around accuracy, validity and bias regarding information found.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

Children are not allowed to download any material from the internet unless directed to do so by an appropriate staff member.

Portable Storage

In the interim, whilst the school develops it's infrastructure towards remotely available desktops, there will be occasions when staff use portable media storage (e.g. USB sticks). If the use of the device results in an anti-virus message, staff should remove the device and report this immediately to the headteacher. Staff will need to ensure that sensitive files (including children's details) are protected by strong passwords. Some materials would be inappropriate to store on portable devices (see staff acceptable use). As a school we distribute Encrypted USB keys to those that require portable data, and that the data is removed after its use has expired.

Mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players. As part of E-Safety teaching within Computer Science, children will be taught the legal and moral implications of posting photos and personal information from mobile devices to public websites and how the data protection and privacy laws apply. Children are not allowed to have personal mobile phones or similar devices in school or during school activities such as trips or residential visits.

Using ICT Safely

Contact details and privacy

Children's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous.

As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based materials. Where pupil websites are published on the wider Internet, perhaps as part of a project, then identifying information will be removed, and images restricted.

Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on children. Our school has a range of strategies and policies to prevent online bullying. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards in school.
- Pupils are taught how to use the Internet safely and responsibly (including awareness regarding age-restrictions), and are given access to guidance and support resources from a variety of sources.
- We encourage children to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.
- Complaints of cyber-bullying are dealt with in accordance with our Behaviour including Anti-Bullying Policy, with the Deputy headteacher taking the lead role.
- Complaints related to child protection are dealt with in accordance with school child protection policy and procedures.
- Acceptable ICT use
- Authorised Access
- All staff, governors and pupils must follow the 'Acceptable ICT Use' sections of this policy.

World Wide Web

If staff, governors or pupils discover unsuitable sites, the URL (address), time, content must be reported to the ICT subject leader or network manager who will block said site.

School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.

Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Social Media

As a school we recognise that social media and networking are playing an increasing role within everyday life and that many staff and governors are users of tools such as Facebook, Twitter and blogs, using these for both personal and professional use. We will ensure that staff, governors and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

As a school we block access to social networking sites on all school computers, unless there is a clear and justifiable need.

Staff and governors should:

- ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc

- not accept current or ex-pupils or parents as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We ask that members of staff take extra care when posting online and maintain professional conduct

- ensure that their communication maintains their professionalism at all times

- be aware that electronic texts can be misconstrued so should endeavour to minimise the possibility of this happening

- not use these media to discuss confidential information or to discuss specific children.

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, individuals may be signed up with, or without, parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will ensure that parents are aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove such accounts or if any issues, such as cyber-bullying occur.

Published Content and the School Web Site

The contact details on the website should be the school address, e-mail and telephone number.

Staff, governors or pupils' personal information will not be published.

The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Digital and Video Images

We follow these rules to maintain safety on our school website and social media:

- For a photograph of a child to appear on the site, consent must have been gained from the parent or guardian of the child. This consent is sought on admission and reviewed annually in September. A parent or guardian may choose to withdraw permission at any time

- If we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure they are not left out of situations unnecessarily

- We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications

- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately

- Personal information about children or staff is not shared on our website. Contact e-mails are provided only for School office, Headteacher, and Website Administrator

- All information on the school website is published by the headteacher or admin team. This avoids content on the website inadvertently contravening these rules

- Photographs of swimming, changing for PE and other instances deemed inappropriate by class teacher will not be taken.

Handling e-Safety Complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the headteacher. The school complaints procedure (published on website) will be used.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Appendices

A. E-Safety Rules for Children

B. ICT Acceptable Use Agreement for Staff

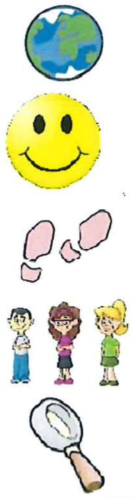
Appendix A – E-Safety Rules for Children

Key Stage 1

Think then Click

These rules help us to stay safe when I go online:

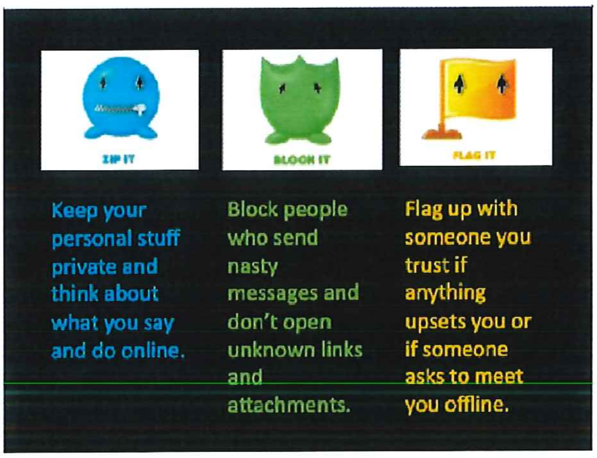
- I only go online with a grown up.
- I am kind online.
- I keep information about me safe.
- I only talk to people online who I know in real life.
- I tell a grown up if something online makes me unhappy.



Key Stage 2

Think then Click

- I ask permission from an adult before using the Internet.
- I only use websites and search engines that an adult has chosen.
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- I will not use technology to be unkind to people.
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission.
- I will immediately close any web page I am not sure about.
- I will never give out personal information or passwords.
- I don't talk to people online unless I know them in real life.
- I never arrange to meet anyone I don't know.
- I have read and talked about these rules with my parents/carers.



Keep your personal stuff private and think about what you say and do online.

Block people who send nasty messages and don't open unknown links and attachments.

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

Appendix B – ICT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-Safety policy for Internet access for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I understand that I must not use the school ICT system to access inappropriate content
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems and hardware may not be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must NOT be kept on removable storage devices.
- I will respect copyright and intellectual property rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidents of concern regarding children's safety to the Designated
    - Safeguarding Lead.
- I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: .... Name: .... Date: ....

Accepted .... Name: ....
for school: