E-Safety

Approved	Feb 16	**Responsibility**	Curriculum Committee
Review	3 years		

This policy is linked to the following:
Teaching and Learning, Inclusion/SEN, Behaviour, PSHE, over arching Safeguarding policy, Child Protection, Equalities policies, Complaints.

Policy prepared	**February 2010**
Policy approved	**March 2010**
Reviewed	**March 2011**
Reviewed	**Feb 2012**
Reviewed	**Feb 2014**
Reviewed	**Feb 2016**
Next review	**Feb 2018**
Review period	**3 Years**

Greenfields Junior School

e-Safety Policy

Writing and reviewing the e-Safety Policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for Teaching and Learning, Inclusion/SEN, Behaviour, PSHE, over arching Safeguarding policy, Child Protection, Equalities policies.

- The school will appoint an e-Safety Coordinator, currently the headteacher, who is also the Designated Safeguarding Lead as the roles overlap.
- Our e-Safety Policy has been agreed by the governors and staff of the school and can be accessed on the school's website.
- The e-Safety Policy and its implementation will be reviewed every 3 years

Teaching and learning

Why internet use is important

- We believe that the internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The internet is an essential element of 21st century life for education, business and social interaction. This school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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, provided at source by our IT provider(HCC)
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Acceptable use agreements signed by all users. (Appendix 1 – Staff Acceptable Use) (Appendix 2 – Pupil Acceptable Use)

Pupils will be taught how to evaluate internet content

- Greenfields Junior School will ensure that all staff and children are aware that the use of internet derived materials should comply with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- The school ICT system's capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Hampshire County Council.

E-mail - Pupils

- Pupils are taught to immediately tell a teacher/an adult they trust if they receive an offensive message.
- Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone without specific permission.

E-mail - Staff

- E-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Staff should use school email address for school related communication

Published content and the school website

- The contact details on the website are 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 pupils' images and work

- Pupils' full names will not be used anywhere on the school website or blog, particularly in association with photographs.
- Photographs that include pupils will be selected carefully. Permission forms are completed by all parents when children enter the school before photographs of pupils are published on the school website. Permission lists are kept in the ICT security folder in the ICT suite and the school office

Social networking and personal publishing

- Hampshire County Council blocks/filters access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that there are a variety of social network spaces outside school. While some are designed for children of primary age, others have age restrictions and therefore are inappropriate.

Managing filtering

- The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator if this is within school.
- The e-Safety Co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and appropriateness before use in school is allowed.
- The use of mobile phones by pupils is not permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff (and the phone left at the school office during the school day).
- Contact with children should be via the school phone only.

Protecting personal data

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

Policy Decisions

Authorising internet access

- All staff and pupils/parents must read and sign the relevant 'E-safety Acceptable Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. This will be found in the ICT security folder in the ICT suite.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor HCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective, particularly in the light of new developments in technology.
- All staff have access to a school laptop, which may be used at home. In these circumstances staff need to ensure they have adequate home insurance in the event of theft or loss. All laptops will be regularly screened for content at least once per year and/or if a member of staff leaves.

Handling e-safety complaints

- Complaints of pupil internet misuse will be dealt with by the appropriate member of staff and the e-Safety Co-ordinator informed.
- Any complaint about staff misuse must be referred to the e-Safety Co-ordinator.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure. O:\Admin Folders\04 Policies\POLICIES\GJS Complaints\GJS Complaints Policy & TOR's Jan 14.doc
- Any breach of these provisions will be dealt with according the severity of the breach. If the breach is a breach of law, the police will be called in straight away and all evidence will be preserved even to the non-use of the school network. If the breach is less severe school disciplinary action would result through established channels.

Community use of the internet

- The school will liaise with local organisations, when appropriate, to establish a common approach to e-safety.

Communications Policy

Introducing the e-Safety Policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and internet use will be monitored.

Staff and the e-Safety Policy

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff can use the school network (which includes internet and e-mail access)
- All staff should immediately report any inappropriate material that appears on their laptop
- The school network can be used at any time that staff are on the premises. The school's internet access is on 24 hours a day and staff can access the internet and e-mail at any time.
- Staff may use the internet or e-mail service for professional or private use (during break times)
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should be aware that all designated laptops will be scrutinised to at least once per year for unauthorised content

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.

Greenfields Junior School
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 policy for internet access for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted
- I understand that it I am unable to communicate information which is confidential to the school or which I do not have the authority to share
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication
- I understand that I must not use the school ICT system to access inappropriate content
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT and is subject to disciplinary action
- 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 follow the school's policy in respect of downloading and uploading of information and material
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.

- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and that activities undertaken are inconsistent with expectations of staff working with children and teacher's standards.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

All staff have read, understood and accepted the Staff Code of Conduct for ICT.

There is a separate pro forma, signed by all staff and kept in the ICT security folder in the ICT suite.

Greenfields Junior School
E-safety Acceptable Use Agreement
Pupil Roles and Responsibilities

Finding information on the internet safely

I know:

- I know that I will be able to use the internet if I use it responsibly
- That being responsible means I should not try to visit unsafe sites or register for things I am not old enough for. There are a variety of social networking sites outside school. While some are designed for children of primary age, others have age restrictions and therefore are inappropriate.
- That any protection system does not stop all unsafe content
- What to do if I open something that I don't like
- How to search safely to find the information I want
- That I should be supervised to ensure I am keeping safe
- That any information I put up on the web can be read by anyone
- That I should ask permission to use the work of others and credit them if I do
- That I should not copy others work and claim it as my own

Using technology to contact people

I know:

- How to choose my user name carefully to protect my identity
- How to keep my personal information private
- How to use safety features of websites
- How to limit access to my information
- That e-mails / messages can be intercepted and forwarded on to anyone
- That I should be careful who I add as friends
- That I need to be polite online and friendly online and think about the language I use (it could be forwarded to my parents or head teacher!)
- How to use the subject field in e-mails
- Not to open messages if the subject field contains anything offensive or if I do not recognise who it is from (delete it without opening it)
- What to do if I receive an offensive message / e-mail including how to keep evidence
- That people online may not be who they seem

Using technology to for buying and selling

I know:

- How to tell the difference between web sites for information and websites selling things
- How to recognise commercial uses of the internet e.g. iTunes, mobile phone downloads, shopping
- Not to leave computers logged on with my user name or logged on to sites with personal details entered
- That if an offer looks too good to be true it probably is
- That I should not respond to online offers
- That I should not use someone else's identity to buy things online

Publishing Children's Work on the School Website

The Greenfields website is used to celebrate work done by pupils in the school and I agree that, if selected, my work may be published using my first name only.

Greenfields Junior School
E-safety Acceptable Use Agreement
Pupil Roles and Responsibilities
Please complete, sign and return to the school

Pupil's Agreement
I have read and understood the school rules for responsible internet use. I will use the computer system and internet in a responsible way and obey these rules at all times.

Signed: _____Pupil

Date: _____

Parent's Consent for Internet Access

I have read and understood the school rules for responsible internet use and give permission for my son/daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet facilities.

Signed: _____Parent/Guardian

Date: _____