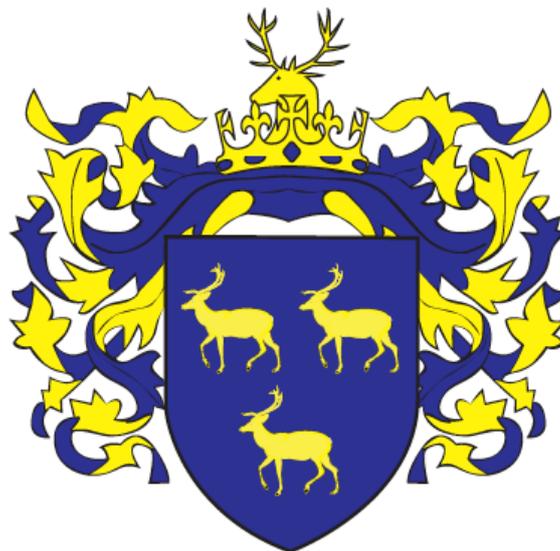# Green Meadow Independent Primary School

E-Safety Policy

Policy approved August 2016
Next review date for policy –August 2018

Robson Way
Lowton,
Warrington
Cheshire WA3 2RD

Manager/Head teacher: Sandra Green
Deputy Head Teacher: Amy Watson
Assistant Deputy Head: Jacqueline Grimshaw

Tel no: (01942 671138)
E-Mail:greenmeadowteachers@gmail.com

School Website:www.greenmeadowindependentprimaryschool.co.uk

Green Meadow Independent Primary School
E-SAFETY POLICY

eSafety

eSafety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's eSafety policy will operate in conjunction with other policies including those for Student Behaviour Management, Curriculum, and Data Protection.

End to End eSafety

eSafety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of eSafety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering.

School eSafety policy

The eSafety Policy is relates to other policies including those for ICT, behaviour management and for safeguarding.

- The school will appoint an eSafety Coordinator. This person is also the safeguarding officer as the roles overlap.
- Our eSafety Policy has been written by the management, building government guidance. It has been agreed by all staff.
- The eSafety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet use is important

- 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.
- 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.
- 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.

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 should 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

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain mail is not permitted.

Published content and the school website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The management team will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or the school social network site, 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's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites for pupils.
- Newsgroups will be blocked unless a specific use is approved.
- 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 the use of social network sites outside school is inappropriate for primary aged pupils.

Managing filtering

- The staff work closely with the eSafety co-ordinator to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the eSafety Coordinator.
- Senior staff 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 a risk assessment will be carried out before use in school is allowed.
- Pupils will not have access to their mobile phones in school. If a child brings in their phone they will need to give it to their class teacher who will store the phone securely until the end of the school day. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where contact with pupils is required.

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 must read and adhere to the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.

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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the eSafety policy is adequate and that its implementation is effective.

Handling eSafety 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 manager.
- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the eSafety policy to pupils

- eSafety 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 eSafety policy

- All staff will be given the School eSafety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School eSafety Policy in newsletters, on the school Web site.

Review

This policy will be reviewed annually or sooner if a change in circumstances or legislation dictates.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key eSafety issues	Relevant websites
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search - Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	EPals SuperClubs PLUS E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum