E-Safety Policy

School: ______________________________

Date adopted by the Governing Body: ______________________________

Review date: ______________________________

Signed by Chair: ______________________________

Signed by Headteacher: ______________________________

THE GRANGE PRIMARY SCHOOL
E-SAFETY POLICY

Introduction

The Grange Primary embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. This policy has been written by the school following the government and LEA guidelines. Comments and consideration from all stakeholders have been used in the formulation of this policy. The e-Safety policy and its implementation will be reviewed annually.

Aims

The Grange Primary School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world. This will occur through:

- A planned e-Safety curriculum in both Computing and PSHE.
- E-Safety messages to be taught through other areas of the curriculum when appropriate.
- During special periods such as Safer Internet Day and other whole school assemblies and events.

Our aim is for e-Safety to be an intrinsic part of the children's education and school life.

Teaching and Learning of E-Safety at The Grange Primary School

The purpose of Internet use in school is to raise educational standards and enhance learning; to promote pupil's achievements; to support the professional work of staff and to enhance the school's management function. In order to achieve these aims teaching and learning will follow these guidelines.

- Key e-Safety messages are reinforced as part of a planned programme of assemblies, the Computing Curriculum, PSHE activities or other curriculum opportunities where appropriate.
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Learners should be helped to understand the need for the NetSmart Code and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Learners should be taught to use search engines safely.
- The NetSmart Code for use of computers is displayed in all rooms and displayed next to fixed site computers.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- All staff will be kept up to date through regular training in e-Safety.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critical of the information they read on the Internet.

Security of Information

The security of the school's information systems will be renewed annually, along with virus protection.
All staff that have been provided with IT equipment, such as laptops and iPads, must ensure that they have a secure password to prohibit others from using it. If there is any doubt of the security of those passwords then they must be changed immediately.
All class teachers, members of the Senior Leadership team and certain members of the administrative staff are provided with encrypted pen sticks for storage of confidential information regarding staff and pupils.
All school email correspondence must be completed using a secure school email address.

School Password

All passwords used by adults should follow the guidelines in this policy:

- No individual should log on using another individual's password, unless they are a member of staff logging on as a child.
- No individual should tell another individual their password.
- Once a computer has been used, users must remember to log off so that others cannot access their information. Users leaving a computer temporarily should lock the screen *(ctrl/alt/del then press K on Windows XP; for Windows 7 and Netbooks, select 'lock' from the Start menu or press ctrl/alt/del and select 'lock'.)*
- Passwords must not be easily guessable by anyone and should ideally be a combination of letters and numbers.
- If you know your password is insecure then it is essential that the password is changed immediately.
- The School's Network Manager and a member of the Leadership Team will have access to all school network drives.

All passwords used by pupils should follow the guidelines in this policy:

- All children have individual log-in details when using the networked computers and accessing their individual educational programmes (such as: RM Easimaths, Lexia and Bug Club).
- No individual should tell another individual their password.
- Once a computer has been used, users must remember to log off so that others cannot access their information.
- Passwords will be stored securely by the Computing Subject Leader and each class teacher will have a copy of their children's log-in details in case a child forgets their details.
- The children will not be able to alter their own password.

Email Use

All pupils have a student e-mail account that works through an internal server and therefore can not be accessed by eternal accounts.
Pupils will also be restricted from sending external e-mails.
Pupils must immediately tell a member of staff if they receive any inappropriate messages from other children.
They must not reveal their password to other students.
Pupils must be reminded that the content of their e-mails must be appropriate.
Excessive social e-mails can interfere with learning and therefore maybe restricted.
Pupils will be expected to behave appropriately when using e-mails **(see Acceptable Use Policy).**

Protection of Personal Data

All personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Policy and Privacy Notices.

Management of Publish Content

The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
The Senior Leadership Team will take responsibility for the published content on the school website and have overall editorial responsibility to ensure the content is accurate and appropriate.
The school's website will respect intellectual property and copyright.
The images of pupils included on the website will have written permission from parents/guardians and will not include full names.

Management of Social Network

The school will block access to social networking sites.
Pupils will be advised on how to stay safe on social networking sites, when accessing them from home, and reminded to follow the NetSmart Code.
Pupils will be advised not to post personal photos on social network spaces.
Guidance on how to strengthen security on social networking sites will be provided for students, staff and parents.

Management of Filtering Systems

The school will work with Sefton Council, a range of outside training facilitators and the school's IT Technician to ensure that systems to protect pupils are in place and are constantly reviewed and improved.
If staff or pupils discover an unsuitable site, the URL must be reported immediately to a member of the Leadership Team or the Computing Subject Leader, who will then take action.
Members of the Leadership Team will ensure that regular checks are made in order to make sure the filter methods being used are appropriate and effective.
Any material that the school believes is illegal must be reported to appropriate agencies such as CEOP.
Computing Subject Leader and members of the Senior Leadership Team, along with the support of the IT Technician, have control over blocking and unblocking of certain sites. Any request to unblock must be reviewed before completion.

Security of Information Systems

The security of the school information systems, will be reviewed annually.
Virus protection will be updated annually by the IT Technician.
Files held on the school's network will be annually checked.
Computing Subject Leader and IT Technician will review system capacity annually.

Loading Software

Only the Computing Subject Leader and IT Technician or a member of the Senior Leadership Team, are allowed to load software on to any school computer.

For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

The only exceptions to this are teacher laptops and iPads, where individuals may download software if they are sure the rules below apply.

Images and video clips may be downloaded as long as the teacher in charge is satisfied that they are not breaching copyright.

Software loaded on to any school system must be: properly licensed; free from viruses and authorised by the Computing Subject Leader, IT Technician or a member of the Senior Leadership Team.

Virus Protection

All computer systems, including teacher laptops, are protected by an Antivirus product which is preferably administered centrally and automatically updated. This is managed by the IT Technician.

Any virus, adware or malware incidents should be reported immediately to the IT Technician.

All USB memory sticks, CDs and other data storage brought to school by pupils should be handed to teachers to complete virus checking procedures in consultation with the Computing Subject Leader or IT Technician before being allowed to be used. The use of these devices are at the discretion of the Computing Subject Leader and the Leadership Team and only if completely necessary.

Internet Access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communication.

All staff must read and sign the Acceptable Usage policy

All pupils in KS1 and KS2 must read and agree to an Acceptable Usage policy.

All parent's and carers must read and agree to an Acceptable Usage policy.

Access to the Internet by pupils will be through adult demonstration, guidance and supervision.

Risk Assessment

The school will take all reasonable precaution to ensure that every user of the Internet will only access appropriate material. However due to the global and connected nature of Internet content, it is impossible to guarantee that access to unsuitable material will never occur. Neither the school nor Sefton Council can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit ICT use on an annual basis to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risk will also be annually reviewed.

Any complaints about the misuse of the Internet will be dealt with by a member of the Senior Leadership Team. Parents will be informed and involved in process until the matter has been concluded.

Protecting Children from Radicalisation

The School will take every reasonable precaution to ensure that filtering systems used at our schools

block inappropriate content, including extremist content.
If staff, pupils or visitors find unblocked extremist content they must report it immediately to a member of the Leadership Team.
Staff will be given training to help them understand the issues of radicalisation, so that they are able to recognise the signs of vulnerability or radicalisation and know how to refer their concerns. This information also forms part of the annual safeguarding training.
Children are made aware through e-safety education that there are inappropriate and extreme messages on the Internet and that they must follow the NetSmart Code and report it, even if it is not during the school day.

Social Networking

For guidance relating to social networking, please refer to the **Social Networking Policy**.

Management of Emerging Technology and Mobile Technology

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
Children who require the use of a mobile phone before and after the school day **MUST** hand it to the class teacher on arrival in school and it will then be locked into the class safe for the entire day. It will be returned to the owner at the end of the day.

Parental Support

Parents/Carers will be given information on the school's E-Safety Policy in newsletters and through the school's website.
Parents will be encouraged to support the school in promoting good e-Safety practice
They will be reminded to follow guidelines on the appropriate use of digital and video images taken at school events, as these are prohibited to be up-loaded on to social media sites.
Parents will be expected to read and sign the Acceptable Use Policy.
Internet issues or complaints will be handled sensitively.

Training

The Computing Subject Leader will attend any e-Safety training provided by Sefton LA and will feedback to the Senior Leadership Team, Governors and other staff in an appropriate forum.
E-safety training audits will be carried out and subsequent training will follow.
Training for other staff, Governors and parents will be provided.
The e-Safety Policy and its up-dates will be presented to and discussed by all staff and Governors.
All new staff will have an e-Safety induction with the Computing Subject Leader to ensure there is a full understanding of the school procedures in this area.

COLLEAGUES WITH RESPONSIBILITY FOR E-SAFETY

Computing Subject Leader – Miss Beverley Wright

Headteacher – Mr. Daniel Hains

Curriculum Manager – Mr. Gwyn Evans

IT Technician – Mr. Stephen Foord