E-SAFETY POLICY

INTRODUCTION

The National Curriculum sets the expectation for children to become digitally literate. It requires children to be able to use, express themselves and develop their ideas through information and communication technology (ICT) in order to prepare them for the future workplace and as active participants in a digital world. It is also a requirement that children are responsible, competent, confident and creative users of ICT.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones, as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguarding and awareness for users to enable them to control their online experience. Grinling Gibbons and Lucas Vale Federation's e-safety policy will operate in conjunction with other policies including those for Computing, Curriculum, Safeguarding and Data Protection.

AIMS OF THE POLICY

The purpose of Internet use in school is to provide the staff, pupils, parents and governors with specific access to the unique educational opportunities it presents. Internet access is an entitlement for children who show a responsible and mature approach to its use.

Knowing that the Internet is an essential element in 21st Century life for education, business and social interaction, the school has a duty to provide children with quality Internet access as part of their learning experience. Considering this, it becomes imperative that we provide guidance on how to use this facility safely, responsibly and efficiently.

ROLES AND RESPONSIBILITIES

The designated e-safety coordinators at Grinling Gibbons Primary School and Lucas Vale Primary School are Foluso Odutuyo and Florida Kranisqu respectively. Both are Computing Leads in their respective schools. The roles and responsibilities of these persons are overseen by the Senior Leadership Team of their respective schools, as well as by the Federation's Consultant Executive Headteacher.

The key responsibilities of an e-safety co-ordinator include:

- developing an e-safe culture
- being the main point of contact on issues relating to e-safety
- putting together and leading an e-safety team
- raising awareness and understanding of e-safety issues amongst all stakeholders, including parents and carers

- embedding e-safety in staff training, continuing professional development and across the curriculum and learning activities
- monitoring and reporting on e-safety incidents to the Senior Leadership Team
- keeping up with relevant e-safety legislations
- liaising with the local authority and other agencies as appropriate
- reviewing and updating e-safety policies and procedures regularly

INTERNET USE TO 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.

TEACHING CHILDREN HOW TO BE SAFE ONLINE

Pupils will be taught, according to their age, how to manage the following risks when using the Internet:

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

In the EYFS children will be taught to:

- recognize that a range of technology is used in places such as homes and schools;
- select and use technology for particular purposes

In KS1, children will be taught:

- use technology safely and respectfully, keeping personal information private;
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In KS2, children will be taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable/unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.
- acknowledge the source of information and to respect copyright when using Internet material in their own work.
- be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- If pupils encounter material they feel is distasteful, uncomfortable or threatening, they should report the address of the site to a member of staff. Pupils will also be taught how to report e-safety incidents outside school by, for instance, reporting to CEOP's website (Child Exploitation and Online Protection) and / or ChildLine.

Schools should ensure that the use of Internet-derived materials by staff and by pupils complies with copyright law and is in accordance with the e-safety policy. Training should be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.

The school's e-safety scheme of work will be embedded in the Computing and PSHE scheme of work.

CYBER BULLYING

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.

By cyber-bullying, we mean bullying by electronic media, including:

- bullying by texts, messages or calls on mobile phones
- the use of mobile phone cameras to cause distress, fear or humiliation
- posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- using e-mail to message others
- hijacking/cloning e-mail accounts
- making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, Youtube and Ratemyteacher, etc.

The school will take any incidents of cyber-bullying involving children or staff seriously. Sanctions to children will be applied in light of the seriousness of the incident and might include, for example, a verbal warning, a formal meeting with parents, confiscation of equipment, detention or exclusion. Sanctions to staff will follow the school's staff disciplinary policy.

REPORTING E-SAFETY INCIDENTS

All e-safety incidents should be reported using CPOMS, the school's safeguarding management system. Staff should select the e-safety area and forward it to their school's e-safety coordinator.
Staff have the right to collect any electronic evidence of cyber-bullying or internet misuse, including confiscation of electronic equipment or a print-screen of website. However, if the evidence has images of a sexual nature or child nudity, no electronic evidence should be recorded or stored and the Head of School should be contacted immediately.
The school will do its best to deal with school-related e-safety incidents which took place outside of the school.

USE OF SCHOOL-RELATED ICT EQUIPMENT OUT OF SCHOOL

Grinling Gibbons and Lucas Vale Federation provides access/use of ICT equipment to staff. Staff members will have access to the Internet and a variety of applications to enhance student learning within the classroom. The policies, procedures and information within this document apply to all equipment and any other IT handheld or mobile device used in school.

User Responsibilities

Users must ensure that they:

- password-protect their ICT equipment and keep it private
- do not subject any ICT equipment to extreme heat or cold
- delete or save photos and videos of children taken in school for learning purposes before taking the ICT equipment out of school premises

The ICT equipment is subject to monitoring by the SLT. Devices must be surrendered immediately upon request by any senior member of staff.

Users in breach of the Responsible Use Policy may be subject to, but not limited to: disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Grinling Gibbons and Lucas Vale Federation is not responsible for the financial or other loss of any personal files that may be deleted from an electronic device.

Lost, Damaged or Stolen equipment

It is a user's responsibility to keep their ICT equipment safe and secure. If any equipment is lost, stolen, or damaged, the Head of School must be notified immediately. Some devices, such as iPads, that are believed to be stolen can be tracked through iCloud. Teachers will be liable for a replacement if due care has not been taken.

Prohibited Uses applicable to school's ICT equipment or personal electronic equipment used in school (not exclusive) are:

- **Accessing inappropriate materials** – All material on the electronic devices must adhere to the ICT Responsible Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- **Illegal activities** – The school's internet/e-mail accounts must not be used for financial or commercial gain, or for any illegal activity.
- **Copyrights** – Users are not allowed to have music and install apps on their electronic devices that violate copyrights.
- **Cameras** – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Images of other people may only be made with the permission of those in the photograph.

DATA PROTECTION

The school collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. Teaching staff are given an encrypted pen drive if they need to take any electronic personal information of children out of school premises. The loss of such pen drive should be communicated to the Head of School immediately.

Teachers are given unique login details to the school's network and these should not be shared with other members of staff.

Children will also be given unique login access to a range of electronic resources and will be educated on how to manage their passwords safely.

MANAGING E-MAIL

The following guidance applies to e-mails in school:

- 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 details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted to certain times during the day.
- Any e-mails 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 letters is banned.

THE MANAGEMENT OF WEB SITE CONTENTS

The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.

Pupils' full names will not be used anywhere on the website, particularly associated with photographs and written permission from parents will be sought before photographs of pupils are published on the school website.

The Head of School or nominee will take overall editorial responsibility and ensure content is accurate and appropriate. The website should comply with the school's guidelines for publications.

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

MANAGEMENT OF NEWSGROUPS AND CHAT SITES

Pupils will not be allowed access to public or unregulated chat rooms. Pupils should use only regulated educational chat environments provided by the school. This use will always be supervised and the importance of chat-room safety emphasised. Newsgroups will not be made available unless an educational requirement for their use has been demonstrated. A risk assessment will be carried out before a new technology is allowed.

MANAGEMENT OF NEW AND EMERGING TECHNOLOGIES

New applications are continually being developed which use the Internet, mobile phone networks, wireless or Bluetooth connections. The user could be mobile using a smartphone or personal digital assistant with wireless Internet access.

Emerging technologies will always be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

MANAGEMENT OF INTERNET ACCCES

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 leaving or the withdrawal of a pupil's access.

At Key Stage 1, access to the Internet will normally be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents will be informed that older pupils will be provided with supervised Internet access. Parents will be asked to sign and return a consent form upon admission.

RISK ASSESSMENT

In common with other media such as magazines, books and video, some materials available via the Internet are unsuitable for children. 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 Federation cannot accept liability for the material accessed, or any consequences of Internet access.

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 risks will be reviewed regularly. The Governors and Head of School will ensure that the Internet policy is implemented and compliance with the policy monitored.

THE FILTERING OF UNSUITABLE MATERIALS

The following technical strategies being developed to restrict access to inappropriate material, fall into several overlapping types (commonly described as filtering):

- **Blocking strategies** prevent access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day.
- **A walled-garden or allow list** provides access only to a list of approved sites. An allow list will inevitably restrict pupils' access to a narrow range of information.
- **Dynamic filtering** examines the content of Web pages or e-mail for unsuitable words. Filtering of outgoing information such as Web searches is also required.
- **Rating systems** give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- **Monitoring** records Internet sites visited by individual user. Access to a site forbidden by the filtering policy will result in a report. It is also possible to remove access automatically after a set number of attempts.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. At Grinling Gibbons, filtering is performed through Firewall by the LA. The school will work in partnership with parents, the LA, DfES and the NGFL to ensure systems to protect pupils are reviewed and improved.

Senior staff will ensure that regular checks are made to ensure that the filtering methods in use are appropriate and effective.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the E-Safety Subject Leader. Any material that the school believes is illegal must be referred to the Internet Watch Foundation. If staff or students require an alternative filtering strategy, an assessment will be made and a new filtering profile designed, where appropriate.

MONITORING

Rules for Internet access will be posted near all computer systems and pupils will be informed that Internet use will be monitored.

All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school. All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet 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. The school ICT systems will be reviewed regularly with regard to security and virus protection will be installed and updated regularly. Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned and files held on the school's network will be regularly checked.

The network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Reviewed by Foluso Odutuyo
January 2017