eSafety Policy

Agreed by:	Martin Ledgard (Head)
Signed:	
Date:	
Review by:	

Contents

1 INTRODUCTION

The purpose of this policy is to safeguard and protect the students and staff of Grange Farm Primary School. We recognise that our children are growing up at a time where the online world is one that is providing increasing potential for learning, enjoyment and communication. However, it is also a world that includes various pitfalls and dangers and children need to be safeguarded against this and taught how to safeguard themselves. Staff need to be aware how to do this, how to safeguard themselves and how to model best practice in their own eSafety behaviours.

2 SCOPE OF POLICY

- This policy applies to all staff and students at Grange Farm Primary School
- Volunteers also need to be aware of their responsibilities
- This policy is a safeguarding document and as such does not stand along but sits amongst a family of associated documents in school including the Child Protection Policy and the Staff Code of Conduct

3 REVIEW AND OWNERSHIP

- This policy has been agreed by the Headteacher, Computing Subject Lead and is subject to review by the Governing Board
- This policy is reviewed annually

4 ROLES AND RESPONSIBILITIES

4.1 The Headteacher (with support from the Computing Subject Lead):

- …is ultimately responsible for the eSafety provision for all members of the community; ensuring that relevant staff receive suitable training to enable them to carry out their roles (and to train other colleagues where necessary)

- …should ensure they are aware of procedures to be followed in the event of a serious eSafety issue
- …should ensure that an eSafety training element will be established as a regular part of annual Child Protection training
- …should ensure that eSafety will be a regular and sustained feature in the school's Computing and wider curriculum
- …should ensure that an effective filtering system is in place to protect children when using the internet in school
- …should ensure that the eSafety policy will be made available to parents / carers

4.2 Teachers:

- …must read, understand, adhere to and help promote the school's eSafety policy, Acceptable Use Policy and guidance
- …should ensure that any digital communications with students should be on a professional level and only through school-based systems
- …should supervise and guide students carefully when engaged in learning activities across all areas of the curriculum
  …should be aware of eSafety issues related to the use of mobile phones, cameras and hand-held devices
- …should report any eSafety related issues to the Designated Safeguarding Lead
- …should ensure that access controls (e.g. passwords) exist to protect personal and sensitive information held on school-owned devices

4.3 Students:

- …must read (or have read to them), understand and adhere to the school's Acceptable Use Policy
- …must understand the importance or reporting abuse, misuse or access to inappropriate materials and know how to do so

4.4 Parents:

- …should consult with school if they have concerns about their children's use of technology that could have an impact in school
- …should support the school's Acceptable Use Policy
- …should support the school's policy on acceptable use of information and photographs by giving or not giving consent for their use on-line

5 STORAGE OF IMAGES

- Any images, videos or sound clips of students must be stored on the school network
- Students and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of students

6 TEACHING AND LEARNING

- Any internet use will be carefully planned to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way
- We will remind students about their responsibilities through an Acceptable Use Policy which every student will consent to when signing on to the school network
- Staff will model safe and responsible behaviour in their own use of technology during lessons
- Staff will review the eSafety Policy annually and will receive update training as necessary and appropriate
- All staff will be made aware of individual responsibilities relating to the safeguarding of young people and know what to do in the event of misuse of technology
- All staff will be encouraged to incorporate eSafety activities and awareness across curriculum activities

7 MANAGING ICT SYSTEMS

- The school will be responsible for ensuring that access to the ICT system is as safe and secure as reasonably possible
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date
- Users will be made aware that they must take responsibility for their use and behaviour while using the delivery provider ICT systems and that such activity may be monitored and checked

8 PASSWORDS

- A secure and robust username and password convention exists for all system access
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available systems available within delivery provider
- Users should change their passwords whenever there is any indication of possible system or password compromise
- No user should be able to access another user's files unless specific permission has been given by a senior manager
- Access to personal data is securely controlled in line with the delivery provider's personal data policy

9 FILTERING INTERNET ACCESS

- The delivery provider uses a filtered internet service. The filtering system will be provided by Coventry Local Authority
- The delivery provider's internet provision will include filtering appropriate to the age and maturity of students
- Any breach of filtering or any unacceptable content must be reported immediately to the headteacher
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-delivery provider requirement across the curriculum

10 EMAIL

- Staff and students should only use approved email accounts (allocated to them by the delivery provider)and should be aware that any use of the delivery provider email system will be monitored and checked
- Staff will only use school-provided email accounts for professional purposes
- Under no circumstances should staff contact students, parents or conduct any delivery provider business using personal email addresses

11 EMAIL USAGE

- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account
- Any inappropriate use of the delivery provider email system or receipt of any inappropriate messages should be reported to a member of staff immediately
- Students must immediately tell a designated member of staff if they receive any inappropriate or offensive emails
- Staff who send emails to parents or students are advised to CC a member of the Senior Leadership Team

12 SOCIAL MEDIA AND ONLINE COMMUNICATION

- Blogging, podcasting and other publishing of online content by students will take place within the school's agreed systems
- Students will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff
- Any public blogs run by staff on behalf of the school will be hosted on the school website and should be approved by the Headteacher or Deputy Headteacher before publishing
- Teachers will model safe and responsible behaviour in their creation and publishing of online content
- Students will be reminded not to reveal personal information which may allow someone to identify and locate them
- Staff and students will be encourage to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other publishing outside delivery provider

13 MOBILE PHONE USE IN SCHOOL

13.1 Staff Use

- Mobile phones will not be used by staff when they are responsible for the care of children. They should be switched off or on a silent mode setting.
- Children should never see a member of staff's personally owned mobile phone or device
- No images or videos should be taken or stored on mobile phones or personally-owned mobile devices
- Mobile phones and personally-owned mobile devices brought in to delivery providers are the responsibility of the device owner. The delivery provider accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices
- There is a school mobile phone for use when required (e.g. on trips)

13.2 PUPIL USE

- No child should have a mobile device in school
- Any devices they have (for example if they need them at the end of the day) should be signed in to the school office for the duration of the school day

14 DATA PROTECTION AND INFORMATION SECURITY

- See the General Data Protection Regulations Policy (renewed for May 2018)

15 MANAGEMENT OF ASSETS

- Details of all delivery provider-owned hardware / software will be recorded in an inventory
- All redundant ICT equipment will be disposed of through an authorised agency. Redundant ICT equipment that may have held personal data will have the storage media overwritten several times to ensure the data is destroyed
- Disposal of ICT equipment will conform to the Waste Electrical and Electronic Equipment Regulations 2006 (or Amendment 2007)