



E-Safety Policy

Reviewed by:	Matthew Walters (Head)
Agreed by:	C. Marscheider
Signed:	
Date:	December 2023



Contents

1 INTRODUCTION	3
2 SCOPE OF POLICY	3
3 REVIEW AND OWNERSHIP	3
4 ROLES AND RESPONSIBILITIES	3
4.1 THE HEADTEACHER (WITH SUPPORT FROM THE COMPUTING SUBJECT LEAD): .	4
4.2 TEACHERS:	5
4.3 STUDENTS:	5
4.4 PARENTS:	6
5 STORAGE OF IMAGES	6
6 TEACHING AND LEARNING	6
7 MANAGING ICT SYSTEMS	7
8 PASSWORDS	7
9 FILTERING INTERNET ACCESS	7
10 EMAIL	8
11 EMAIL USAGE	9
12 SOCIAL MEDIA AND ONLINE COMMUNICATION	9
13 MOBILE PHONE USE IN SCHOOL	10
13.1 STAFF USE	10
13.2 PUPIL USE	10
14 DATA PROTECTION AND INFORMATION SECURITY	10
15 MANAGEMENT OF ASSETS	11



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. The school also makes volunteers aware of their responsibilities. This policy is a safeguarding document and as such does not stand alone 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. It is reviewed annually.

4 ROLES AND RESPONSIBILITIES

The Governing Board:

The Governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff



understand their expectations, roles and responsibilities around filtering and monitoring.

The Governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Headteacher (and Senior Leaders):

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Headteacher should ensure they are aware of procedures to be followed in the event of a serious eSafety issue and ensure that an eSafety training element will be established as a regular part of annual



Child Protection training. Alongside the Computing Lead, the Headteacher will ensure that eSafety will be a regular and sustained feature in the school's Computing and wider curriculum and that an effective filtering system is in place to protect children when using the internet in school. The Headteacher will ensure that the eSafety policy will be made available to parents and carers.

School staff:

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

In the event of being made aware of a 'sharing of nudes and semi-nudes' type incident (formerly known as 'sexting') they inform a DSL of the incident in a timely manner, record relevant details on CPOMs and refer to guidance as necessary.

Students:

All student must read (or have read to them), understand and adhere to the school's Acceptable Use Policy. They must understand the importance or reporting abuse, misuse or access to inappropriate materials and know how to do so. Students must understand that incidents relating to cyber-bullying and/or online that occur outside of school, will be investigated and acted upon in school. Students will be educated about the benefits and the risks associated with the use of social media and will be taught how to remain safe online. Students agree that they will not use any personal mobile phone or technology (including smart watches) on school site and must hand in any such devices at the start of the school day to the office.



Parents:

Parents play an important role in ensuring that their children understand the need to use technology and the internet safely. Parents should consult with school if they have concerns about their children's use of technology that could have an impact in school. Parents are expected to support the school's Acceptable Use Policy and the school's policy on acceptable use of information and photographs by giving or not giving consent for their use on-line. The school will work with parents to provide up to date information to support parents to ensure their child is kept safe online.

5 STORAGE OF IMAGES

All school staff are aware that any images, videos or sound clips of students must be stored securely on the school network. Students and staff are not permitted to use personal portable media or mobile phones 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 and also engage in other opportunities such as Safer Internet Day.

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

At Grange Farm 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 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 school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented.

It will also ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:



- All users will have clearly defined access rights to school ICT systems;
- All users will be provided with a username and password for the school network. This includes teachers, teaching assistants, other designated staff and all pupils in key stages 1 and 2. A central record of all passwords used on the school systems will be kept;

The school is currently using a filtering service provided by Impero. This blocks any sites containing banned words or which come under predetermined categories. Any attempts to access such sites, or the typing of unacceptable words, triggers a screen shot which is sent to a central log. These are then checked by the ICT co-ordinator. Where such screen shots require a follow up investigation, the Headteacher will be informed; Requests from staff for websites to be removed from the filtered list will be considered by the ICT co-ordinator and members of the SLT. The removal, if approved, will be completed by the school IT support staff;

The Headteacher and the ICT co-ordinator can monitor the activity of users on the school ICT systems, and users are made aware of this in the Acceptable Use Policy. Staff are forbidden from installing programmes on school workstations / portable devices without written permission from the ICT Co-ordinator or Headteacher (any such installation requires administrator login. The school infrastructure and individual workstations are protected by up to date virus software. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured and as per the Acceptable Use Policy, users may only store pupil and sensitive data on the school server, Microsoft Sharepoint, or on encrypted memory sticks that are provided by school.

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.

Parent/Teacher email communication is sent through the admin email account.

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

Social media are being used increasingly to fuel campaigns and complaints against schools, Headteachers, school staff, parents and pupils. Grange Farm Primary School considers the use of social media in this way as unacceptable and not in the best interests of the children or the whole school community. Any concerns must be made through the appropriate channels by speaking to the Class Teacher, the Headteacher or the Chair of Governors so that they can be dealt with fairly, appropriately and effectively. The school's complaints procedure is available online via the school website.

In the event that any pupil or parent/carer of a child being educated at Grange Farm is found to be posting libellous or defamatory comments on



Facebook or other social network, they will be reported to the appropriate 'report abuse' section of the network site or other appropriate action will be taken where messages from forums such as Whatsapp are reported to school. All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this. The school will also expect that any parent/carers or pupil removes such comments immediately. In serious cases, the school will also consider its legal options to deal with any such misuse of social networking and other sites. Additionally, and perhaps more importantly, is the issue of cyber bullying. In the event of any member of the school community using social media to publicly humiliate another by inappropriate social network entry, we will deal with this as a serious incident of bullying.

13 MOBILE PHONE USE IN SCHOOL

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.

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 handed into the school office for the duration of the school day.

14 DATA PROTECTION AND INFORMATION SECURITY

See the GDPR Policy.



15 MANAGEMENT OF ASSETS

Details of all delivery provider-owned hardware / software will be recorded in an inventory and managed by the school ICT provider. 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. The disposal of ICT equipment will conform to the Waste Electrical and Electronic Equipment Regulations 2006 (or Amendment 2007)