Online Safety Policy

Ratified by Governors
October 2021

Date for Review
October 2022 (or earlier if required)

Chair of Governors
Katie Atkinson

Head Teacher
Daniel Kerbel

Introduction

The purpose of this document is to provide a basis for us all to secure safety when using digital technology and when working online. This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling online bullying and it also refers to the Department's guidance on protecting children from radicalisation. It should be considered alongside complementary school policies on Child Protection, Health and Safety, Home-School Agreement and Behaviour (including the Anti-bullying policy). This policy applies to all members of Grange Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of Grange Primary School. The implementation of this policy seeks to ensure that children stay safe, and that they be protected from harm, neglect and extremism and grow up able to look after themselves. (*Ref: KCSIE 2021- The 4 key categories of risk)*
This policy establishes clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate. School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place in or out of school. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

All members of the school community have a responsibility for Online Safety.

The resources used by pupils at Grange Primary School are usually carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its very nature, will occasionally provide access to information which has not been selected by the teacher - particularly as children reach the later years of Key Stage 2. Within the school and our wider community, there is genuine cause for concern that children may access unsuitable material either accidentally or deliberately.

The Internet and other digital and information technologies are powerful tools that open up new opportunities for everyone. We believe that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. We feel that the best recipe for success lies in a combination of site-filtering, supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Roles and Responsibilities

Role	Key Responsibilities
Head teacher	• To take overall responsibility for Online Safety provision. • To take overall responsibility for data and data security (SIRO). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL. • To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious Online Safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator/Officer. • To ensure that there is a system in place to monitor and support staff who carry out internal Online Safety procedures (e.g. Network Manager).

Online Safety Co-ordinator / Designated Child Protection Lead	• To take day to day responsibility for Online Safety issues and take a leading role in establishing and reviewing the school online safety policies/documents.
	• To promote an awareness and commitment to e-safeguarding throughout the school community.
	• To ensure that Online Safety education is embedded across the curriculum.
	• To liaise with school ICT technical staff.
	• To communicate regularly with SLT and the designated Online Safety Governor/Committee to discuss current issues, review incident logs and filter/change control logs.
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.
	• To ensure that the Online Safety incident log is kept up to date.
	• To facilitate training and advice for all staff.
	• To liaise with the Local Authority and other relevant agencies.
	• To seek guidance from The Prevent Duty when concerns of extremism are raised.
	• To keep up-to-date on Online Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal/inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media
	  • extremism
	Ref: KCSIE 2021- The 4 key categories of risk)

Governors /Online Safety governor/ Child Protection	• To ensure that the school follows all current Online Safety advice to keep the children and staff safe.

Role	Key Responsibilities
governor	• To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors/Governors Sub-Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. • To support the school in encouraging parents and the wider community to become engaged in Online Safety activities. • The role of the Online Safety Governor will include: • regular review with the Online Safety Co-ordinator/Officer (including reviewing Online Safety incident logs and filters)
Computing Curriculum Leader	• To oversee the delivery of the Online Safety element of the computing curriculum. • To liaise with the Online Safety Co-ordinator regularly. • To liaise with the Network Manager regarding managing, monitoring and filtering Google Classroom and live online learning. • To communicate with parents and provide Online Safety advice. • To arrange and manage Safer Internet Day.
Network Manager	• To report any Online Safety related issues that arise to the Head teacher/DSL/Computing Curriculum Lead. • To ensure that users may only access the school's networks, Google Classroom and other online learning portals through an authorised and properly enforced password protection procedure. • To ensure that provisions exist for misuse detection and malicious attack e.g. keeping virus and malware protection up to date. • To ensure the security of the school ICT system. • To ensure that access controls/encryptions exist to protect personal and sensitive information held on school-owned devices. • To ensure the school's policy on web filtering is applied and updated on a regular basis. • To ensure LGfL is informed of issues relating to the filtering applied by Webscreen 3. • To ensure that he/she keeps up to date with the school's Online Safety Policy and technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant. • To ensure that the use of the network/online learning platforms/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher for investigation/action/sanction. • To ensure appropriate on-site and cloud backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To contact LGFL and Google for further information.
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts.
Teachers	• To embed Online Safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaging in learning activities involving online technology (including extra-curricular and extended school activities if relevant).

Role	Key Responsibilities
	• To set Online Safety tasks on Purple Mash to refresh and update children's awareness. • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. • To teach children the SMART rules for the internet. • To be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites.
All staff	• To read, understand and help promote the school's Online-Safety policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use Agreement Policy. • To be aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices, to monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to Network Manager. • To maintain an awareness of current Online Safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• To read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents/carers would sign on behalf of the pupils). • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking/use of images and on cyber-bullying. • To understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • To help the school in the creation/ review of Online Safety policies. • To know the SMART rules.
Parents/carers	• To support the school in promoting Online Safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video

Role	Key Responsibilities
	images. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children. • To access the school website/online learning platform/online pupil records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology.
External groups	• To sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Using the Internet for Education

The benefits include:

- access to a wide variety of educational resources including libraries, art galleries and museums, that can stimulate discussion and promote creativity;
- rapid and cost effective world-wide communication;
- gaining an understanding of people and cultures around the globe;
- staff professional development through access to new curriculum materials.

At Grange, we teach pupils about the vast information resources available on the Internet, using it as a planned aspect of many lessons. All staff will review and evaluate resources available on websites appropriate to the age range and ability of the pupils being taught and the ICT Curriculum Leader will assist in the dissemination of this information.

Initially the pupils may be restricted to sites that have been reviewed and selected for content. They may be given tasks to perform using a specific group of websites. Pupils may have the opportunity to exchange information with others via email, however, access to public chat rooms and social networking sites is prohibited and therefore blocked by the schools filtering system.

As pupils gain experience, they will be taught how to use searching techniques to locate specific information for themselves. Comparisons will be made between researching from different sources of information such as CD ROMs, books and the World Wide Web. We hope that pupils will learn to decide when it is appropriate to use the Internet as opposed to other sources of information, in terms of the time taken; the amount of information found; and the usefulness and reliability of information located.

Grange Primary will use London Grid for Learning's (LGfL) actively monitored and 'filtered' Internet Service, which will minimise the chances of pupils encountering undesirable material. Loaned devices have HomeProtect software installed for safeguarding and monitoring purpose. If staff or pupils discover unsuitable sites, the URL (web address) and content will be immediately reported to the Internet service provider via the IT Network Manager and will be blocked within a short period of time. We will only ever allow children to use the Internet when there is a responsible adult present to supervise them. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, on a regular basis, the expectation we have of them. Rules for Internet access will be posted near computer systems. The 'Rules for Responsible Internet Use' could be printed as posters. Teachers and educators will have access to pupils' workspaces, and will make periodic checks on a regular basis to ensure expectations of behaviour are being met.
AB Tutor has been installed on all of the PC's and laptops in the school. AB Tutor is used to monitor the Internet usage and to update/troubleshoot the devices. Any security breaches detected is reported to the Safeguarding officer and/or to the Head teacher.

At times, information (including photographs and images), may be downloaded from carefully selected Internet sites for use in pupils' presentations. As children become older, tasks will be set to encourage pupils to view websites and information with a critical eye. However, Grange Primary specifically discourages the downloading of text for inclusion in pupils' work. This includes inclusion of such text for homework projects! As well as encouraging pupils to create original work and avoid plagiarism (a serious academic offence), Grange Primary considers it appropriate to emphasise the importance of protecting intellectual property rights and, in particular, copyright.
Pupils will be made aware of these issues and, as soon as they are able, will be encouraged to look for copyright information on websites, so reinforcing their understanding of the importance of copyright.

(Ref: KCSIE 2021- The 4 key categories of risk)

The main areas of risk can be summarised as following:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language)
- lifestyle websites
- hate sites
- content validation

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online - internet or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Expectations for Internet use

- We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school.
- Unless instructed to by a member of staff, pupils must always ask permission before using the Internet and have a clear idea why they are using it.
- Pupils and staff should never reveal personal details, home addresses and telephone numbers on the web or in dialogue with other Internet users.
- Children will not engage in any form of conversation or dialogue with other users on the Internet without permission and supervision from their teacher. This may only occur in Google Classroom with closely guarded passwords.
- The use of public Instant Messaging Services is prohibited.
- The use of social networking sites such as Snapchat, Facebook, TikTok, Instagram, MySpace etc are not generally appropriate to primary education and the use of the Internet for such purposes is not currently permitted.
- The use of personal technology such as mobile phones, cameras, CD's and memory sticks is prohibited.
- Computers should only be used for school work and homework.
- Files may only be downloaded by staff, or pupils under supervision.
- Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any such material be encountered accidentally, or if any child finds themselves uncomfortable or upset by anything they discover on the Internet, they will report it to the supervising adult. Any adult should report it to the IT Network Manager or Head Teacher immediately. Arrangements can then be made to request that the Internet Service Provider blocks the site.

In EYFS and KS1, children may log on using a year group login, but in KS2 pupils should generally only access the network using their own personal login. No network user should access other people's files unless permission has been given.

Any infringement of these conditions of use will be dealt with by the Class Teacher/Head Teacher/IT Network Manager as appropriate and sanctions may apply. Parents will be informed.

School Website Guidelines

A website can celebrate good work, promote the school, publish resources for projects and homework, and link to other good sites of interest. However, to protect our children, the following guidelines will be adhered to:

- Photographs or videos of pupils will only be used on the website or the school's official social media channels with parental consent and in full clothing. A parent or guardian may request for an image or video featuring their child to be removed from the site/social media platforms at any time.
- No full names or other identifying information will be attached to photographs.
- The content of pictures should be considered for good taste and the dignity of people in the pictures.
- Pupil's work displayed online will be identified only by their first name and will not contain information such as family names, which might identify that pupil or family members. Nicknames which would not identify the pupil may be allowed.
- Any incident of an image considered by a pupil, staff member or parent to have been inappropriate for the website or violation of these guidelines should be reported to the Head teacher. The person reporting may choose to do so anonymously, but must give reasons why they feel the image is not appropriate.
- Teacher's pages must not contain: CVs and personal messages; non-job related personal information; personal opinions about school policy or related controversial issues; personal contact details.
- Governing Body and Parent Teacher Association pages should not contain personal contact details of members.
- Pupil or class pages are generally created as class learning resources and assignments. However, they must nevertheless be checked to ensure that they do not contain personal contact information about the student, including email addresses.
- Pupil or class pages must not include links to their own or other pupils' personal websites containing personal contact information or materials and contents contrary to the Pupil Acceptable Use Policy or these guidelines.
- Events and trips should contain general information only.

Parents who would prefer that their children do not appear on our school website are asked to inform the school office in writing. An up-to-date list of such children is kept in the school office and referred to before new pages are added. If, at any time, a parent expresses concern about usage of an image or piece of work, it will be removed from our site as quickly as possible.

Online Learning Platform

As our community moves towards use of an online learning platform (Google Classroom), it is important to note that any user who accesses this provision will be expected to agree to an Acceptable Use Policy before access is granted. As online reporting and parental engagement develops, our Online Safety guidelines will be reviewed.

Pupil Acceptable Use of Policy

No pupil is allowed to use a mobile phone during school hours/trips and so Internet access should only occur via the school networks whilst on school premises. The use of personal technology such as cameras, CD's and memory sticks is also strictly prohibited.

Information and further guidance for parents:

We have done all we can to ensure children are protected through the use of a filtered service and a requirement that an adult always supervises Internet access. Our children are taught to use the facility sensibly - the rules concerning Internet use are regularly discussed in class and we welcome your endorsement of these. We strongly recommend that parents consider and develop a similar set of rules for the use of the Internet outside of school. You might also like to discuss as a family the issues surrounding the downloading of music, mobile phones, social networking sites, and the use of blogs, within the home environment. You may find the following websites useful to help ensure that children stay safe.

Childnet International is a non-profit organisation working to help make the Internet a great and safe place for young people. These sites are all created by this organisation.

http://www.childnet-int.org http://www.kidsmart.org.uk http://www.chatdanger.com

You can find downloadable safety leaflets here:

http://www.childnet-int.org/downloads/parents-leaflet.pdf

http://www.childnet-int.org/downloads/musicLeaflet.pdf

http://www.childnet-int.org/downloads/ICRA-Bill-of-Rights.pdf

http://www.childnet-int.org/downloads/a2poster.pdf

Other useful sites include:

NSPCC	https://www.nspcc.org.uk/
Parent Zone	http://parentzone.org.uk
Safe Kids	http://www.safekids.com
Cyber Patrol	http://www.cyberpatrol.co.uk
Net Nanny	http://www.netnanny.com
CBBC	http://www.bbc.co.uk/cbbc/help/safesurfing (aimed at KS1)
Bullying Online	http://www.bullying.co.uk
Think U Know	http://www.thinkuknow.co.uk

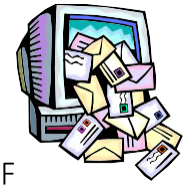
BECTA: Safeguarding children in a digital world; LGFL- Online safety & Safeguarding

Online Safety Policy Appendices

Can be found on the following pages:

Key Stage One Acceptable Use Policy	12
Key Stage Two Acceptable Use Policy	13
Parent Acceptable Use Policy	14 - 15
Social Media Policy	16 - 19
Staff Acceptable Use Policy	20 – 22
Glossary	23 - 24

Think before you click!

S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	I will close the page and tell an adult when I feel unsafe.

My Name:

My Signature:

The 12 Rules for Responsible ICT use

These rules will keep me safe and help me to be fair to others.

1. I will only use the school's computers for schoolwork and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into school without permission or upload inappropriate material to my workspace.
5. I am aware that some websites and social networks have age restrictions and I should respect this.
6. I will not attempt to visit Internet sites that I know to be banned by the school.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
11. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it and I will call my teacher/ additional adult.

I have read and understand these rules and agree to them.

Signed: …… *Date:* ……

Grange Primary School Online Safety agreement form: Parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter(s) or son(s) to have access to use the Internet, LGfL e-mail*, Google Classroom and other ICT facilities at school.

I know that my daughter or son has signed an Online Safety agreement form and that they have a copy of the '12 Rules for responsible ICT use' (KS2) or the 'Think before you click' form (KS1).

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching Online Safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their Online Safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's Online Safety.

Parent / guardian signature: _____

Date:____/___/____

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature:_____**Date:**____/___/____

Grange Primary School
Use of digital images - photography and video

To comply with the Data Protection Act 2018, we need your permission before we can photograph or make recordings of your daughter / son.

We follow these rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first name, rather than their full name.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that the pupil's full name isn't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, educator or another child) as part of a learning activity;
  E.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school;
  E.g., in school wall displays and PowerPoint presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  E.g. within a CD-ROM / DVD, Social media; in our school prospectus or on our school website. In rare events, your child could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Social Media Policy

Ratified by Governors

Date for review
October 2022 (or earlier if considered necessary)

Chair of Governors
Katie Atkinson

Head Teacher
Daniel Kerbel

Introduction

The principles set out in this policy are designed to ensure that the use of social media among the Grange Primary School community is undertaken responsibly and that the confidentiality of students and staff and the reputation of the school are safeguarded.

Scope

This policy applies to Grange Primary School students, staff, parents and the wider school community. It covers personal use of social media, as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

This policy applies to personal web space such as social networking sites (for example Facebook, Instagram, Snapchat, TikTok), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.ico.us and content sharing sites such as Flickr and YouTube.

Since it is impossible to cover all circumstances of emerging media, the principles set out in this policy should be followed irrespective of the medium.

Related Policies

Code of Conduct
ICT Policies
Acceptable Use Policy (IT)
Safeguarding Policy
Terms of Agreement

Guidelines for Students

- Your online behaviour should reflect the same standards of honesty, respect and consideration that you use face to face.
- Your use of social media should be age appropriate e.g. only over 13's should be using Facebook.
- When posting comments or photos on social media channels, ask yourself whether you would be happy for your parents to read the posts.
- Provide as little information about yourself as possible; not providing your date of birth or location will improve your online security.
- You should set your privacy settings to friends only but be aware that if your friend's settings are not the same as yours, your posts may be seen more widely.
- Think carefully before engaging with strangers in "open" environments, especially Twitter and be aware that "protecting" your tweets will improve your online security.
- Do not attempt to "friend" or "follow" staff on social media sites.
- Do not tag or identify yourself (or other students) on Grange Primary School social media sites; even when using your own accounts, you should ask permission before tagging someone in a photo.
- Do not engage in any activities involving social media which might bring Grange Primary School into disrepute.
- Do not engage in any abusive, threatening, unkind or bullying behaviour.
- Use of profanity or threatening language is not acceptable.
- Under no circumstances should negative comments be made about staff, parents or other students on social media sites.
- Grange Primary School reserves the right to monitor social media activity and if students are found contravening the guidelines, the school sanctions will be imposed.

Guidelines for Staff

- You should decline friend requests and/or block follows from students or parents/carers you receive in your **personal** social media accounts.
- You should not accept any contact from a former student of the school if they are under the age of 18.
- You should not have contact with a student's family members through personal social media if that contact is likely to constitute a conflict of interest.
- Do not take photos or videos with your own phone, camera or tablet – the school has equipment available for this.
- If posting a photograph on an approved school social media platform, do not use the student's full name if they are in the photo. You may only use their full name if no photo is used, or the post is referencing something that has already been published about the student and is well known e.g. a notable prize-winner
- Do not tag photos of staff or students.
- When using a hyperlink in any social media, check that the content is appropriate, especially if you are sharing it.
- Do not discuss personal information about other pupils, Grange Primary School and the wider community you interact with on any social media.
- You should set your privacy settings on Facebook to friends only but be aware that unless your friend's settings are the same as yours, your posts may be seen more widely.
- Passwords and other login information must be kept safely, remember to lock your workstation when you leave it unattended.
- School email addresses should not be used to set up personal social media accounts or to communicate through such media.
- All email communication between staff and members of the school community should be made from official school email accounts
- Do not engage in activities involving social media which might bring Grange Primary School into disrepute.
- If you are aware of any inappropriate communications involving any student in a social media situation, please report it to a member of SLT.
- If in any doubt regarding issues relating to specific students, please check with a member of SLT.

Guidelines for Parents

- The school will monitor and where appropriate, moderate content and activity on Grange Primary School's social media platforms.
- The school cannot be held responsible for improper use of social media by students.
- It is the responsibility of parents/guardians to monitor the child's activity on social media.
- If you do not wish for your child's name or photograph to be used in connection with the school's official social media platforms, website or PR, you must advise the school.
- We ask that any comments posted on the school social media accounts are constructive and not seen as a vehicle for questions that require immediate response or negative comments or complaints which should be referred directly to the school office.

Social Media for Marketing

If you have any concerns about content you have viewed on social media sites, you should contact office@grange.harrow.sch.uk.

While staff and the wider community are encouraged to interact with these social media sites they should do so with responsibility and respect.

Monitoring Internet Use

Grange Primary School monitors usage of its internet, online content, online services and email services in line with AUP, ICT, Social Media and Safeguarding policies.

Users of Grange Primary School email and internet services should have no expectation of privacy in anything they create, store, send or receive using the schools ICT system.

Breaches of this Policy

Any breach of this policy that leads to a breach of confidentiality, defamation or damage to the reputation of Grange Primary School or any illegal acts or acts that render Grange Primary School liable to third parties may result in legal action, disciplinary action or sanctions in line with the published school policies for staff and pupils.

Name of School	**Grange Primary School, Harrow**
AUP review Date	**October 2021**
Date of next Review	**October 2022**
Who reviewed this AUP?	**HT/SLT/NM**

Acceptable Use Policy (AUP): Staff agreement form

The school has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers and technology are provided and maintained for the benefit of all staff. You are encouraged to use and enjoy these resources, and help to ensure they remain available to all. However, if resources are used inappropriately they will be withdrawn and there will be disciplinary action.

Equipment

- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.

- Staff will immediately need to report any damage or fault involving equipment or software to the Network Manager however this may have happened.

- It is strongly recommended that school laptops, computers, iPads and emails are used for school use only. However, if they are used for private use this should be as limited as possible, of a suitable nature and such usage should be outside of work hours.

- Staff are not permitted to use portable hard drives or USBs on the school network.

- Staff are not permitted to connect personal mobile equipment (e.g. laptops, tablet PCs, iPads etc.) to the school network without express permission from the Headteacher/SLT/Network Manager.

- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

- Staff are not permitted to use personal ICT (i.e. smartphones, cameras) for teaching purposes and should not use these devices to take pictures or videos of pupils at any time.

- Regulations for the use of ICT equipment off-site (i.e. school trips or staff working from home) follow the same instruction as on site.

One copy is retained by the member of staff Second copy is retained by the IT Network Manager

- Inform the Network Manager if you wish to have any software or apps installed on the school computers/laptops or iPads.

- Staff will be asked to submit their assigned IT equipment from time to time to the Network Manager for updates and other maintenance work.

Security and Privacy

- Protect your work and safeguard sensitive documents by making sure to lock your workstation when away from your desk; access should only be made via your given username and password, which should not be made available to anyone else.

- General Data Protection Regulations requires that any information seen by the staff with regards to staff or pupil information, held within the School's Information Management System (SIMS), will be kept private and confidential, unless it is deemed necessary that they are required by law to disclose such information to an appropriate authority.

- Teachers will ensure that they are aware of digital safeguarding issues so that these are appropriately embedded in their classroom practice.

- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.

- Other computer users should be respected and should not be harassed, harmed, offended or insulted.

- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk and can lead to disciplinary action.

- IT staff may review your computer usage to ensure that you are using the system responsibly.

- When sensitive or personal data is required by an authorised user from outside the school's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or Online learning platform (G Suite)

- Council policy requires the use of a specific whole-disk encryption on any laptop, which is used to store confidential data.

Internet

- Staff should access the Internet only for school activities during work time.

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

- ‘Chat’ activities take up valuable resources, which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons use of ‘chat’ rooms are not allowed.

- Members of staff should be wary of compromising their professional standing through inappropriate use of social media ensuring that any private social networking sites / blogs etc. that they create or actively contribute to are not confused with their professional role.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.

- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer and compromise the whole school network.

- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of SLT and Network Manager. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden and is monitored.

- Staff e-mail and Internet use is also filtered for the safety of all members of staff.

Please read this document carefully. Only once it has been signed and returned to the Network Manager access to the school network will be given. If you violate these provisions, access to the school network will be denied and you will be subject to disciplinary action. Access to LGFL emails, shared drives and personal drives can be accessed at any time on request from SLT during or after employment has ended.

Additional action may be taken by the school in line with the existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Signature: ……. Date: ……

Name: … ……

One copy is retained by the member of staff Second copy is retained by the IT Network Manager

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by Naace
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
KS1	Key Stage 1 (2, 3 or 4) – schools are structured within these multiple age groups e.g. KS2 = years 3 to 6 (age 7 - 11)
LA	Local Authority

LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. LGfL) to provide the safe broadband provision to schools across Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (e.g. LGfL) have been established to procure broadband connectivity for schools in England.
SEF	Self-Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self-Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICT Mark
LGfL	London Grid for Learning – the Regional Broadband Consortium of Local Authorities – is the provider of broadband and other services for schools and other organisations in the London area
TUK	Think U Know – educational Online Safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol