



Grosvenor Road Primary School

Online Safety, Mobile Technology & Acceptable Use Policy (incl. use of Google Classroom)

Signed:

Headteacher _____

Date _____

Chair of Governors _____

Date _____

Online Safety & Mobile Technology Policy

Online 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, providing safeguards and awareness for users to enable them to control their online experience.

The previous online safety Policy has been revised to reflect the change in how people use technologies to educate, communicate, work and socialize, in a rapidly changing world.

The school's online safety policy will operate in conjunction with all other school policies.

1. Writing and reviewing the Online Safety and Mobile Technology Policy

The online safety policy is part of the School Development Plan and relates to all other school policies including those for computing, bullying and for safe guarding/child protection.

- Our Online Safety and Mobile Technology Policy has been agreed by the Senior Leadership Team, staff and approved by governors.
- The Online Safety and Mobile Technology Policy and its implementation will be reviewed annually.

2. Teaching and learning

Why Internet use is important

- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- It states in the UN Rights of the Child – Rights respecting article that,

Article 17 (Access to information: mass media): *Children have the right to get information that is important to their health and well-being. Governments should encourage mass media – radio, television, newspapers and Internet content sources – to provide information that children can understand and to not promote materials that could harm children. Mass media should particularly be encouraged to supply information in languages that minority and indigenous children can understand. Children should also have access to children's books.*

Yet the schools Online Safety and Mobile Technology Policy should further underpin these rights by ensuring pupils are taught how to stay safe online and that they have a right to privacy as stated in

Article 16 (UN Right of the Child – Right to privacy): *Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.*

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils, as well as use of online platforms (RMUnify, Senso and Google classroom) to guide pupils to use and explore specific relevant websites.
- 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. To further enhance pupils safe use whilst searching the internet, pupils will use the search engine www.swiggle.org.uk .

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
 - Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy: such as cross-referencing information from different sites; assessing the trustworthiness from a site's address - .org, .gov, .co.uk, bbc etc.

3. Areas of risk for our school community.

Content

- Exposure to inappropriate content, including online pornography, hate promotion, ignoring age rated content, extremist views and terrorism.

Contact

- Grooming
- Online bullying in all forms – including WhatsApp, Snapchat, TikTok, YouTube etc)

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation.

4. Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is regularly updated remotely by RM – Managed Service.
- RM advise on appropriate security strategies.

Social networking and personal publishing

- The school blocks/filters access to all social networking sites.
- Newsgroups are blocked unless a specific use is approved by the HT and then the LA
- Pupils will be advised never to give out personal details of any kind which may identify them or their location, on any platform they use.
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary pupils.

Managing filtering

- The school has filtered internet access through RM Education SafetyNet, which are members of the Internet Watch Foundation (IWF).
- The school will work with the LA, RM and Salford ICT Services to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the ICT Coordinator DHT and HT.
- The HT, DHT and Online Safety and Mobile Technology Policy lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Half termly checks of the filtering and monitoring reports produced by RM Education safetynet will be undertaken by the Online safety and Mobile Policy lead.

Filtering and monitoring in school

The latest update to the statutory guidance Keeping Children Safe in Education 2023 ('KCSIE 2023') now includes reference to the DfE's filtering and monitoring standards. The standards, which were published on 29 March 2023, are intended to support schools to meet their duty and to have appropriate/effective filtering and monitoring systems in place.

To meet these standards, Grosvenor Road Primary School will:

1. Identify and assign roles and responsibilities to manage the filtering and monitoring systems.
2. Review the filtering and monitoring provision at least annually.
3. Ensure the filtering system blocks harmful and inappropriate content without unreasonably impacting teaching and learning.
4. Implement effective monitoring strategies that meet the safeguarding needs of our school.

All school devices, including individual children's Chromebooks, are part of the school's Senso Monitoring program. The system monitors keyboard entry and reports key words and watch words as they are typed on any child's keyboard. This provides real time and highly effective monitoring of all users on the school system. This should provide parents and carers with confidence that their children's experience of the online world is safe and backed up by a broad curriculum of online safety guidance.

E-mail

- Staff have email accounts and must make sure that they change their password and do not divulge it to anyone for security reasons. If they have any worries about their account they must see the Online Safety and Mobile Technology Policy lead, DHT or HT.

Published content

School web site

- The contact details on the school website are the: schools address, e-mail and telephone number. Staff or pupils' personal information are not published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names are not used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published; permission will also be sought informally from children themselves.

Mobile phones and devices.

- The school policy is that children should not bring mobile phones or any form of electronic communication devices to school. (see full Mobile Phone Policy on school website)
- Mobile phones will not be used during lessons or formal school time but the correct usage will be discussed with children as part of anti-bullying and PSHE curriculum.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff recording images, video and audio on any mobile phone or non-school device is not permitted.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises, where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Managing emerging technologies

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

Policy Decisions

Authorising Internet access

- At Key Stage 1 and 2, pupils will be directly supervised when accessing specific, approved on-line materials.
- Parents, pupils and staff will be asked to sign and return an Acceptable Use Policy (Please see AUPs attached).
- The HT reserves the right to refuse network access to any member of staff or pupil who breaches the AUP.

Assessing risks

- 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 school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit computing provision to establish if the Online Safety and Mobile Technology Policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection/safeguarding nature must be dealt with in accordance with school's child protection procedures.
- Pupils and parents are informed of the Complaints Procedure.

Failure to comply

- Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by the Headteacher and Online Safety and Mobile Technology Policy Lead.

5.

6. Communication of Policy

Pupils

- Online safety rules are posted around the school and will be discussed with the throughout the year.
- Pupils are informed that network and Internet use will be monitored.

- Pupils are shown how to access www.thinkuknow.co.uk which supports of all ages in keeping themselves safe online.
- Promotion of online safety policy themes takes places each year in February during Safer Internet Day.
- Pupils sign an agreed online safety charter for each class each year during safer internet week in February.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.

Staff

- All staff are given the Online Safety and Mobile Technology 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.

Parents

- Parents' attention will be drawn to the Online Safety and Mobile Technology Policy in newsletters, the school brochure and on the school Web site.
- Questionnaires are sent out to parents, at parents evening, to gauge parental awareness and pinpoint their needs with online safety issues. From there, online safety sessions will be put in place, if needed, for parents.
- If necessary, parents will be approached individually if the school has any concerns regarding a pupil's use of the internet.

How we raise children's awareness of online safety

Children are taught:

1) Electronic technologies are fun

Using the internet is a really fun way of keeping in touch with friends and family sending and receiving images, music, texts and streamed video.

There are lots of ways of doing this including IM, chat rooms, and through playing games and writing in blogs and on social network sites. Mobile phones are now an everyday part of life that are becoming increasingly like a hand-held computer.

2) How you can stay safe when you are using the internet

Staying safe is about knowing that some people use the internet to be nasty to others, either to bully or groom.

We discuss issues including:

- Chatting.
- IM.
- Email.
- Mobile Phones.
- Chat Rooms.
- Social media / networking.
- File Sharing.
- Gaming.
- Peer on peer abuse
- Trolling.
- Cyber Bullying - The use of phones, instant messaging, e-mail, chat rooms or social networking sites such as Facebook and Twitter to harass threaten or intimidate someone for the same reasons as stated above.
- Sexting - Sexting is when someone sends or receives a sexually explicit text, image or video. This includes sending 'nude pics', 'rude pics' or 'nude selfies'. Pressuring someone into sending a nude picture can happen in any relationship and to anyone, regardless of their age, gender or sexual preference.

3) What to do if you feel threatened or upset online

Being online and using the internet is just like being in the real world - you can chat to people, play games and share pictures. But sometimes things happen which can make you upset. People may say nasty things to you which upset you, or you may see something that you don't like.

If this happens, you must remember that it's not your fault.

- ALWAYS TELL A TRUSTED ADULT straight away if you are upset or worried about something that has happened online.
- Remember to SAVE ANY MESSAGES that have upset you so you can show them to who you tell - they will be able to help, and they will be able to give you good advice about what else you can do. Never worry about getting in trouble - you aren't the one who has done anything wrong.
- If you don't want to talk to a trusted adult, you may want to chat to someone else about how you feel. THERE4ME IS A SITE WHERE YOU CAN HAVE A PRIVATE ONE-TO-ONE CHAT with someone from the children's charity NSPCC.
- CALL CHILDLINE FREE ON 0800 1111. You can talk to someone in private and it won't show up on your phone bill.
- You can also report any issues / people by using the report button / dropdown or when you see the CEOP button / image.

FURTHER INFORMATION

Useful Documents and Resources

Childnet:	www.childnet.com
Kidsmart:	www.kidsmart.org.uk
Safe Social Networking:	www.safesocialnetworking.com
Digizen	http://old.digizen.org/cyberbullying/default.aspx (cyber bullying)
NSPCC	www.nspcc.org.uk
UKCCIS	Sexting in schools and colleges Advice on child internet safety 1.0 Universal guidelines for providers Online safety in schools and colleges: Questions from the Governing Board
DfES/BECTA	Superhighway Safety
DfES/QCA	The Primary National Curriculum In England 2013
BECTA	Safeguarding children in a digital world
Signposts to safety:	Teaching e-safety at Key Stages 1 and 2 - www.thinkuknow.co.uk Child Exploitation and Online Protection (CEOP) Centre

STAFF ACCEPTABLE USE AGREEMENT/CODE OF CONDUCT

This agreement document is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT in school and as part of the professional role. All staff are expected to sign this agreement document and adhere at all times to its contents. Any concerns or clarification should be discussed with the School's Online Safety and Mobile Technology lead.

- I will only use the school's email / Internet / Network and any related technologies for professional purposes or for uses deemed 'reasonable by the Head Teacher / Governing Board.
- I will not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload or send material that could be considered offensive or illegal.
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Head Teacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's Online Safety and Mobile Technology Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature Date

Full Name



Pupil Acceptable Use Agreement and Google Classroom Code of Conduct



This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following  **I WILL** and  **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.



I WILL:

- treat my usernames and passwords like my toothbrush – I will not share them, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- immediately report any damage or faults involving equipment or software, however this may have happened



I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- try to use any programmes or software that might allow me to bypass the filtering /security systems in place to prevent access to such materials
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes on any device, or store programmes on a computer
- **try to alter computer settings**

Pupil Acceptable Use Agreement and Google Classroom Code of Conduct

This form relates to the pupil Acceptable Use Policy (AUP) and Google Classroom Code of Conduct, to which it is attached.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action, if I am involved in incidents of inappropriate behaviour covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include: loss of access to the school network/internet and loss of break times. Parents will be contacted and, in the event of illegal activities, there may be involvement of the police.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, Google Classroom Learning Platform, website, blog etc.

Name of Pupil		
Class		
Signed (Pupil)		Date

PAPER COPY – will be signed in school by pupil and retained in school office

(Parents and Carers also sign this form as part of the Consent and Agreement Pack
- issued when their child joins Grosvenor Road Primary School).