Online Safety Policy

Introduction

Key people / dates

Great Moor Community Infant School	Designated Safeguarding Lead (DSL)	Yvonne Dobson Liz Stephenson
	Deputy Designated Safeguarding Lead (DSL)	Diana Heis Eve May
	Online-Safety Lead (if different)	Yvonne Dobson
	Online-Safety / Safeguarding link governor	Estelle Buckley Helen Pechey
	PSHE Lead	Lucy Lightburn John Lucas
	IT Support	AVA Support
	Date this policy was reviewed Policy Author	September 2021 Emma Ash (Computing Lead)
	Date of next review and by whom	September 2022 Emma Ash / Yvonne Dobson

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside the statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Writing and reviewing the Online Safety Policy

- This Online Safety Policy has been written by building on information sourced from the Internet and government guidance. It has been agreed by staff and approved by the governing body.
- The school has appointed an Online-safety Lead and the Designated Safety Lead also supervise policy content.

What are the main online safety risks today?

Online-safety risks are categorised as one of the ***3 Cs: Content, Contact or Conduct*** (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas

remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation and it is important to understand the interplay between all three. Many of these new risks are mentioned in KCSIE 2021.

Teaching and learning

Why the Internet and digital communications are important?

- The Internet is an essential element of life today for education, business and social interaction.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Our school provide pupils with internet access as part of their learning experience.
- As pupils use the internet widely outside school they need to learn how to take care of their own safety and security.
- The use of the internet in school is to raise educational standards, including pupil achievement and to support the professional work of staff.

How does internet use benefit education?

Benefits of using the internet in education include:

- Access to worldwide educational resources and learning including museums and art galleries.
- Professional development for staff through access to educational materials and effective classroom practice.
- Collaboration across networks of schools, support services and professional associations.
- Exchange of curriculum and administration data with Stockport Local Authority.

Internet use will enhance learning

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to infant age pupils to enhance and extend education.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.
- Staff will guide pupils to online activities that support their learning outcomes.
- Pupils will be educated in the effective use of the internet including navigation.
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to respond to unpleasant content

- Pupils and staff will be taught to report unpleasant internet content to a member of staff who will notify the Online Safety Lead. They will contact the network support team to have the site filtered.

Managing Internet Access

Published content and the school web site

- Staff or pupil personal contact information will not generally be published.
- The contact details on the website are the school address, email and telephone number.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- All parents or carers sign forms on entry giving or with-holding permission for photographs to be published in school publications, online platforms and within the classrooms and around school.
- Pupils' full names will not be used anywhere on a school Web Site or other online platforms, particularly in association with photographs.
- Pupil image file names will not refer to the pupil by name.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic devices.

Social networking and personal publishing

- GMCIS have formed their community group within Facebook, to share school news and information with parents/carers. This is closely monitored by staff members.
- We do not allow pupils ANY access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of family/friends, specific interests and clubs.
- Parents will be advised that the use of social network spaces outside school brings a range of dangers for infant aged pupils.
- Parents and staff are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff will adhere to the rule that any friend request from a child or parent in their school must NOT be accepted. Equally no staff should request friendship with a current pupil or parent.

Managing filtering

- The school will work with Stockport Local Authority and the school's support team (AVA Support) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Head Teacher or DSL.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (Internet Watch Foundation) or Child Exploitation and Online Protection Command (CEOP).

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.
- The staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The Remote Learning Policy outlines how Google Classroom should be used appropriately.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read and sign the "Staff Code of Conduct for Network & Internet Use (acceptable Use Policy)" before using any school IT resource.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- On entry to the school Parents/Carers will be given access to the Pupil & Parent Acceptable Use Policy and a will to give consent via the Teacher2Parent App.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Stockport Local Authority can accept liability for any material accessed, or any consequences resulting from of Internet use.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by the Head Teacher or Chair of Governors. Staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure (see schools complaints policy).
- Pupils and parents/carers will be informed of consequences for pupils misusing the Internet.
- All online safety complaints and incidents will be recorded by the school – including any actions taken.

Community use of the Internet

- The school will be sensitive to internet related issues experienced by pupils out of school.

How will cyberbullying and 'sexting' be managed?

Cyberbullying (along with all forms of bullying) and 'sexting' also known as youth produced sexual imagery) will not be tolerated in school. At the time of writing this policy, no cyberbullying or 'sexting' has ever been reported at Great Moor Community Infant School. However, should an instance occur, the following will take place:

- Support for anyone affected by these incidents.

Cyberbullying

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying possible witnesses, and contacting the service provider if necessary.
- Sanctions for those involved in cyberbullying may include: The bully will be asked to remove any material deemed to be inappropriate or offensive Service provider may be contacted to remove content. Internet access may be suspended at school for the user for a period of time. Parent/carer may be informed.

Sexting

- Act in accordance with school safeguarding and child protection policies and procedures.

Communications Policy

Introducing the online policy to pupils

- Online safety rules are discussed with pupils at the beginning of each academic year, with frequent reminders.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Online safety will be embedded within the Computing scheme of work or the Personal Social and Health Education (PSHE) curriculum covering both safe school and home use.

Staff and the Online Policy

- All staff and governors will have access to the School Online Safety Policy and its importance explained.
- To protect all staff and pupils, the school will implement acceptable use policies.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School online Policy in the school brochure and on the school Web Site.
- The school will ask all new parents/carers to sign the parent /pupil agreement when they register their child with the school.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats. The public sector equality duty of the Equality Act 2010 has been considered in the writing of this policy. A Discrimination Impact Assessment concludes that through this policy Great Moor Community Infant School seeks to:
- Eliminate discrimination, harassment and victimisation and other conduct prohibited by the

Act.

• Advance equality of opportunity between people who share a protected characteristic and those who do not.

• Foster good relations between people who share a protected characteristic and those who do not. Protected Characteristics: age, disability, gender, gender identity, race, religion or belief, and sexual orientation.

Useful resources for teaching staff:

Teaching online safety in schools	https://www.gov.uk/government/publications/teaching-online-safety-in-schools
Common Sense Education	https://www.commonsense.org/education/
Child Exploitation and Online Protection Command	https://www.ceop.police.uk/CEOP-Reporting/
Childline	https://www.childline.org.uk/
Think UKnow	https://www.thinkuknow.co.uk/
Digiduck Stories	https://www.childnet.com/resources/digiduck-stories
Project Evolve	https://projectevolve.co.uk/

Useful resources for parents/carers:

Internet Matters	https://www.internetmatters.org/
Parent Info	https://parentinfo.org/
LGfL	https://www.lgfl.net/online-safety/default.aspx
Digital Parenting	https://www.vodafone.co.uk/mobile/digital-parenting
Net Aware	https://www.net-aware.org.uk/
Childnet	https://www.childnet.com/parents-and-carers/parent-and-carer-toolkit
Guide to age ratings	https://www.bbfc.co.uk/about-us/news/bbfc-launch-parents-guide-to-age-ratings

Appendix:

Online Safety Audit	Yes/No	Action
Has the school got an Online Safety Policy that complies with BCC guidance?	y	
Date of latest update (at least annual).	y	
Date the school online policy was agreed by governors.	y	
The policy is available for staff on the staff shared network in school.	y	
The policy is available for parents/carers on the school website.	Y	
Name of the responsible member of the Leadership Team.	Y	
Has online safety training been provided for both pupils and staff where appropriate?	Y	Further staff training Jan21
There a clear procedure for a response to an incident of concern.	Y	
Online safety materials from CEOP and Becta been obtained if appropriate.	Y	
All staff sign an Acceptable Use Policy - Code of Conduct for Network and Internet Use.	Y	
All pupils aware of the School's Online safety Rules.	Y	
Parents/carers will adhere to the Pupil & Parent/Carer Acceptable Use Policy, an agreement that their child will comply with the School Online Safety Rules.	Y	
Staff, pupils, parents/carers and visitors are aware that network and Internet use is closely monitored and individual usage can be traced.	Y	
If personal data is collected, stored and used is this according to the principles of the Data Protection Act?	Y	

Pupil Acceptable Use Policy Agreement Information for Pupil's & Parents/Carers

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate effective learning. At Great Moor Community Infant School we believe the children have an entitlement to safe Internet access at all times.

This policy is intended to ensure that: children will be responsible users and stay safe whilst using the Internet and other communications technologies for educational, personal and recreational use; and, that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the system or users at risk.

Great Moor Community Infant School will try to ensure that the pupils will have good access to IT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement - Pupil

I understand that I must use school computers, iPads, Chromebooks and other technologies in a responsible way - so that myself and others keep safe. I will use the Online Safety rules in school to keep me safe.

For my personal safety:

- I will be aware of "stranger danger" when I am on-line.
- I will not give any of my own personal information, or personal information about my family and friends when I am on-line.
- If I see something that makes me feel sad or upset I will tell an adult I know and trust.
- I will treat my username and passwords like my toothbrush – I will not share it or use anyone else's.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the technologies (Chromebooks / iPads etc.) are for school work and will not use them for anything else without the permission of a staff member.
- I will not damage any school equipment on purpose.

I will be kind to others:

- I will use kind words on-line.
- I will not take photos of anyone without their permission.
- I will not copy, delete or change other people's work, unless I have been told to.

I will help school to keep everyone safe:

- I will not bring my own communication technologies into school without permission.
- I will tell an adult if I see anything that is broken.
- I will not try to download programmes or apps.

When using the Internet:

- I will use only websites / programs / apps that my teacher tells me to use.
- If I am finding information I will try to check that the information is the truth.
- I will not copy other people's work, unless I have permission.

I understand that I am responsible for what I do both in and out of school:

- I understand that the school may take action if I do not follow the above rules in school and out of school (if it affects the school or any other pupil / staff member). This may include my parents / carers being contacted.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you would like further explanation of these rules, please contact the school.

The online safety rules are displayed around the school, in classrooms and within the building. These have been shared with the pupils.

Acceptable Use Policy Agreement – Parent/Carer

As the parent/carer of the above pupil, I give permission for my child to have access to the internet and to IT systems at school. I know that my child has been talked through the Acceptable Use Agreement. They will receive an online safety education as part of the Computing and PSHE curriculum to help them understand the importance of safe use of IT – both in and out of school. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies. I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

By giving your consent to GMCIS you are adhering to the Acceptable Use Policy on behalf of your child and yourself as the parent/carer.

If you would like to sign a paper copy please contact the school office.

At Great Moor Community Infant School we can stay safe!

Staff Code of Conduct for Network and Internet Use – Acceptable Use Policy

The purpose of this Acceptable Use Policy Agreement is to provide clear information about safer working practice, keeping your personal and professional lives separate, keeping yourself safe when using electronic media and adopting behaviour that will protect you from putting yourself at risk.

To ensure that all Staff is fully aware of their professional responsibilities when using computers and on line systems in and out of school, they are asked to sign this code of conduct. Staff should consult the school's Online Safety Policy, Image Use Policy & Remote Learning Policy for further information and clarification.

Effective Practice

1. Set your privacy settings for any social networking site to ensure only the people you want have sight / access to the contents. Keep these regularly updated as some sites occasionally reset them. Most social networking sites are set to open access where anyone can see everything.
2. Where possible, ensure personal electronic equipment such as a mobile phone is password/PIN protected.
3. Make sure that any information about you that is publicly available that you are aware of is accurate (Google yourself to find what is publicly available). If you don't want it to be public, don't put it online. Ask for it to be removed.
4. Be mindful about how you present yourself when you are publishing information about yourself or having conversations online. Remember these may be referred to as 'chat' but they are written documents and should always be treated as such.
5. If you are unsure who can view online material, assume that it is publicly available. Remember - once information is online you have relinquished control of it. Other people may choose to copy it, to edit it, to pass it on and to save it.
6. Switch off or password protect any Bluetooth capability on personal electronic equipment. Bluetooth could allow another person to have access to your equipment.
7. Respect copyright and intellectual property rights

What I know and what I will do:

- I am familiar with the 1. Online Safety Policy; 2. Image Use Policy; 3. The Remote Learning Policy; 4. The Parent/Pupil acceptable Use Policy and I understand my responsibilities.

- I will not give my personal information to children/ young people or their parents/carers. This includes mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords.

- I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner (computers and tablets are school property).

- I will inform the designated Child Protection Officer in school about any encounters that worry me.

- I will ensure that my use of the network and information systems will always be compatible with my professional role.

- I understand that any online activity should not harass, harm, offend or insult other users.

- I understand that if/when using CC4 Anywhere (CITREX server) Remote Access from home, this will be appropriately and for its intended purpose.

- I will ensure that any personal or sensitive information I access (e.g. SIMs data, assessment data) is kept secure and used appropriately.

- I understand that school information systems and the Internet may be used for school and personal interests where these do not conflict with the ethos and interests of the school but not for any other private purposes, without specific permission from the Head teacher.
- I understand that the school may monitor my use of the Network and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate person.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. I will do so by using an encrypted device to ensure compliance with the Data Protection Act
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school following the flowcharts set out in the school Online Safety Policy
- I will ensure that any electronic communications with pupils/parents/carers are compatible with my professional role.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will promote the prevent strategy and help children's resilience to resist the influence of extremism and radicalisation.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published and publicly accessible (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- When I use personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using a PC.
- I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not mention school or school staff in relation to work on any social media sites.
- I will not use my personal mobile phone during lesson times or when children are present. It will be switched off unless special permission has been given.
- I will not take photographs or videos of pupils with any personal devices.

- I will make sure that any personal device that is brought onto the school site is my responsibility to ensure that these items contain nothing of an inappropriate nature.

Use of mobile phones – taken from School Safeguarding Policy 2021

Mobile phones have a place in settings, especially on outings when they are often the only means of contact available to settings and can be helpful in ensuring children are kept safe.

We will:

- Only use mobile phones appropriately, and ensure staff have a clear understanding of what constitutes misuse and know how to minimise the risk.
- Ensure the use of a mobile phone does not detract from the quality of supervision and care of children.
- Ensure all mobile phone use is open to scrutiny.
- Ensure staff are vigilant and alert to any potential warning signs of the misuse of mobile phones.
- Ensure staff are responsible for their own behaviour regarding the use of mobile phones and understand how to avoid putting themselves into compromising situations, which could be misinterpreted and lead to potential allegations.
- Ensure the use of mobile phones on outings is included as part of the risk assessment, for example, how to keep personal numbers that may be stored on the phone safe and confidential.
- Adhere to the school policy on the recording of images and the use of equipment (Image Use Policy 2021)

<u>Work mobile phones</u>
To protect children, we will ensure that the work mobile:

- Is only used by allocated people.
- Is protected with a password/ PIN and clearly labelled.
- Is stored securely when not in use.
- Is not used in areas such as toilets, changing rooms, nappy changing areas and sleep areas.

<u>Personal mobile phones</u>
To protect children, we will ensure that personal mobiles:

- Within classrooms personal mobile devices are stored securely in lockers/drawers or bags, switched off whilst staff are on duty.
- Are not used to take pictures of the children attending the setting or that images are not shared.
- Will not be used to take photographs, video or audio recordings in our setting.
- Are not used to contact parents or children – exception will only be by agreement with the SLT.

Visitors are not permitted to use mobile phones or other camera/ internet enabled devices without the express permission of the Headteacher.

I have read, understood and agree with the School's Code of Conduct.