**Great Moor Junior School e-safety policy**

**Updated July 2023 for September 2023**

**Introduction**

**All staff and pupils are encouraged to use critical thinking with all online content and we all together ensure it is monitored, such that all staff and pupils know how and to whom to raise concerns.**

**All staff and pupils are sensitive to good practices when online**

This document provides advice and guidance to ensure safe working practice. It is about **everyone’s** conduct and professionalism.

**Staff**

It is about keeping **your** personal and professional lives separate, keeping **yourself** safe when using *digital media* and adopting responsible behaviour that should protect **you** from putting **yourself** at risk.

**Pupils**

It is about how to protect and safeguard children/pupils in our care and what to do if, and when any incident arises.

The safeguarding and promotion of the welfare of children is a priority.

‘Staying safe’ means that children and young people are:

* safe from maltreatment, neglect, violence and sexual exploitation
* safe from accidental injury and death
* safe from bullying and discrimination
* safe from crime and anti-social behaviour in and out of school
* safe from extremists’ material and radicalisation influence
* secure, stable and cared for.

For further details on Safeguarding see **GMJS Safeguarding Policy** and **Keeping Children Safe in Education 2022**

**Governing Body**

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such, they will:

* Review this policy at least annually (and review it in response to any e-safety incident) to ensure that the policy is up to date; covers all aspects of technology use within the school; to ensure e-safety incidents have been appropriately dealt with; and ensure the policy was effective in managing those incidents.
* Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
* Keep up to date with emerging risks and threats through technology use.
* Receive regular updates from the Head teacher in regards to training, identified risks and any incidents.
* Chair the e-Safety Committee

**Head teacher**

Reporting to the governing body, the Head teacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer, as indicated below.

The Head teacher will ensure that:

* E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
* All e-safety incidents are dealt with promptly and appropriately.

**e-Safety Officer**

The day-to-day duties of e-Safety Officer is devolved at present to Mark Gill and Bob Breckwoldt.

The e-Safety Officer will:

* Keep up to date with the latest risks to children whilst using technology; be familiar with the latest research and available resources for school and home use.
* Review this policy regularly and bring any matters to the attention of the Head teacher.
* Advise the Head teacher, governing body on all e-safety matters.
* Engage with parents and the school community on e-safety matters at school and/or at home.
* Liaise with the local authority, IT technical support and other agencies as required.
* Retain responsibility, along with Head teacher, for the online **e-safety incident log (**in Staff shared area);
* Ensure staff know to report any issues in the **class behaviour online book** in staff shared area and any issues will go in the **e-safety incident log.** This will ensure the appropriate audit trail.
* Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviourmanagement software) are fit for purpose through liaison with the local authority and COMPUTING Technical Support.

**COMPUTING Technical Support Staff**

This policy also affects any technical staff that works in and on our school COMPUTING infrastructure and software. (They must agree to it too and sign it as if they are a member of staff*)*

Technical support staff (at present MGL) are responsible for ensuring that the school’s IT infrastructure is secure; to do this will include at a minimum:

* That anti-virus is fit-for-purpose, up to date and applied to all school and capable devices.
* Windows updates are regularly monitored and devices updated as appropriate.
* Any e-safety technical solutions such as Internet filtering are operating correctly and include filtering of inappropriate materials, such as extremist groups.
* Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Head teacher.
* Passwords are applied correctly to all users regardless of age
* Passwords for staff will be a minimum of a mix of letters and numbers and a minimum length of 6 items.
* The IT System Administrator password is to be changed a minimum of once per year.

**All Staff**

Staff will ensure that:

* All details within this policy is understood and that if anything is not understood, it should be brought to the attention of the Head teacher.
* Any e-safety incident is reported to the Head teacher (and an e-Safety Incident report is made to be put in the e-safety incident log – held by the Head Teacher), or in their absence to the Deputy Head teacher. If you are unsure about whether it is an incident for reporting, see the e-Safety Officer or the Head teacher to make a decision.
* The reporting flowcharts below contained within this e-safety policy are fully understood.

**All Pupils**



 The boundaries of use of COMPUTING equipment and services in this school is set out in the pupil **Acceptable Use Policy**; any deviation or misuse of COMPUTING equipment or services will be dealt with in accordance with the school’s behavior policy.

E-Safety is embedded into our curriculum with regular, planned and progressive lessons/opportunities for developing pupils’ knowledge and skills along with any necessary and appropriate advice and guidance by staff. Similarly, all pupils will be fully aware through discrete lessons and PSHE how they can report areas of concern whilst at school or outside of school. We are following guidance set out in “Teaching Online Safety in School” June 2019 DfE-00128-2019 and Education for a Connected World. Computing discrete e-safety lessons use this via lessons from **Project Evolve**

**Be Smart**

The focus of e-safety is the use of the Be Smart acronym (as used by Childnet International and Kidsmart), which has been rolled out across the school since January 2016. This was chosen by the pupils’ e-safety representatives at the time.

**Parents and Carers**

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge, they need to ensure the safety of children outside the school environment. Through parents’ evenings (lead by the E-safety officer or experts from the Local Authority or outside agencies), school newsletters, and other leaflets, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered to make responsible and safe choices.

Parents must also understand the school needs to have rules in place to ensure the safeguarding of their child. Parents will co-sign with their child/children, the pupil’s Acceptable Use Policy before any access to school COMPUTING equipment or services, on commencing the school in Year 3, or whenever they join the school.

**e-Safety Committee**

Chaired by the Governor responsible for e-Safety, the e-safety Committee is responsible for the following:

* To advise on changes to the e-safety policy.
* To establish the effectiveness (or not) of e-safety training and awareness in the school.
* To recommend further initiatives for e-safety training and awareness at the school.

Members will include at least the e-Safety Officer, the responsible Governor and one other from the staff/parents to meet in person or online on a termly basis.

**Technology**

Great Moor Junior School uses a range of devices including PC’s, laptops, cameras, iPads and Apple Macs. In order to safeguard the student and in order to prevent loss of personal data, we employ the following technology:

**Internet Filtering** – we use SmoothWall software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites. Appropriate and inappropriate is determined by the age of the user, is agreed by the head teacher and IT services and will be reviewed in line with this policy or in response to an incident. The COMPUTING Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head teacher. If a member of staff wishes to unblock appropriate sites they should contact/liaise with the e-safety officer, IT Manager or the Head Teacher.All reasonable precautions are made to ensure that users access only appropriate material

**Email Filtering** – school emails are provided through a secure website using Gmail which is provided, managed and supported by MGL. It prevents any infected email to being sent from the school, or to be received by the school. Infected email is email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

**Encryption & Data Security**

Portable devices (Laptops and PCs) will use encrypted USB memory sticks for any data that needs protecting or the laptop will be encrypted. Our technician must be notified if you want the laptop encrypted.

Portable storage media (USB memory sticks, portable hard drives CD's and DVD's) that are needed for taking sensitive data off site are encrypted. All teachers have one encrypted USB memory stick.

Any device storing data and used outside of the secure space will be encrypted.

Any data no longer required should be securely deleted.

Data transmitted between systems and locations is be encrypted.

Encryption solutions used are of an accepted standard as advised by our technical support.

All school devices that hold personal data (as defined by the Data Protection Act 1998 and the **General Data Protection Regulation** (**GDPR**) are encrypted

No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB memory sticks) is to be brought to the attention of the Head teacher immediately. The Head teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner’s Office.

**Remote Access-** Staff using Remote access to school servers from home must ensure the laptop, PC or other device they use is password protected and has sufficient and up to date virus and internet protection software installed. They must not save any sensitive pupil information on these personal devices.

**Passwords** – all staff and students will be unable to access any device (except the school iPads for pupils) without a unique username and password.

**Staff passwords will change if there has been a compromise, immediately afterwards.** The COMPUTING Coordinators and IT Support will be responsible for ensuring that passwords are changed.

**Anti-Virus** – All capable devices will have anti-virus software. This software will be updated regularly for new virus definitions. Our technical support will be responsible for ensuring this task is carried out, and will report to the Head teacher if there are any concerns. All USB peripherals such as key drives are scanned by Symantec Endpoint Protection when installed, to be scanned for viruses before use.

**Google Classroom-** The use of Google Classroom for home learning and home works must be done following the Google Classroom protocols drawn up for GMJS and available in the staff shared folder. These lay out clear protocol of use for staff, parents and pupils.

**Safe Use**

**Internet** – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the e-safety policy and the staff **Acceptable Use Policy**; students upon signing and returning their acceptance of the **Acceptable Use Policy**.

Pupils will be taught and shown through lessons and example good online activities and practices e.g. responsible use of the Internet to investigate and research school subjects, cross-curricular themes or topics related to social and personal development

**Pupils** will:

* Follow the rules (**Pupil AUP - Acceptable Use Policy**) for Internet access; they are displayed near all computers
* Be helped to understand the need for the Pupil AUP
* Have equal access to use of the internet in a safe and secure environment.
* Will be taught about responsible use of the Internet, World Wide Web and e-mail.
* Will be aware of the Be Smart advice.

**All Staff** will:

* Use their authorised account and have a password that should not be made available to any other person, except at the discretion of the head teacher
* Ensure sites and materials accessed are appropriate to work in school.
* Not use own cameras or mobile devices for storing images from school
* Be responsible for all e-mail sent and for contacts made that may result in e-mail being received.
* Maintain the same professional levels of language and content are applied as for letters or other media, particularly as e-mail is often forwarded
* Know that posting anonymous messages and forwarding chain letters is forbidden
* Respect copyright of materials and intellectual property rights, not plagiarising others’ work
* Ensure that all Internet use should be appropriate to staff professional activity or to student's education
* act as good role models in their use of the Internet, computers and mobile devices
* Planned e-safety programme is provided as part of the Computing curriculum and is updated regularly to reflect changes in the use of online and digital devices in and out of school
* Staff may use the internet for school and personal interests (including shopping) where these do not conflict with the ethos and interests of the school or their professional responsibility
* Any user wishing to download files and programs should ask the school technician to do so. This is to ensure protection of the network as well as in terms of software and licence conflict and cost.
* Reserve the right to check all disks/memory sticks, or any other portable electronics storage device that are brought in to be used on the network or on any standalone machine.
* Use for personal financial gain, gambling, political purposes or advertising is forbidden.
* Will not mention school, pupils or school staff in relation to work on any social media sites

**Email** – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted using the school email system. Personal email addresses for work purposes is not permitted.

Pupils have access to class emails and the virtual email system used within the VLE

School email uses Gmail which goes through a secure socket.

**Photos and videos** – Digital media such as photos and videos are covered in the schools’ Photographic Policy. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

**Social Networking** – there are many social networking services available; at present no social media services are permitted for use within our school, but this will be regularly reviewed and if the school agrees to use any they will be appropriately risk assessed.

Should staff wish to use other social media, permission must first be sought from the Head teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

**Mobile Phones -**All **school** mobile phones are barred from calling premium rate numbers and any numbers outside of the UK by default. **Staff** should not be using personal mobile phones in school during working hours when in contact with children. They should be switched off during this time unless given specific permission.  **Children** are not allowed mobile phones in school.

**Networked Computers -** All staff ensure that any screens are locked (use  + L ) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access. A default timeout of 30 minutes has been set.

**Videoconferencing –** the school uses Google Classroom for videoconferencing. There are Staff parents and pupil protocols (see Protocols in Staff Shared area –Policies). All staff follow the Remote Learning Policy and Remote Learning Risk Assessment.

**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, and the view of the IT services and our technical support shall be sought.

**Any other technology**

**Staff:** know that privately owned equipment should never be connected to the school’s network without the specific permission of the Head teacher or COMPUTING co-ordinators;

**Children** should not bring in their own equipment unless asked to do so by a member of staff.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

In addition, if any agreement is made then the following is to be strictly adhered to:

* Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
* There is to be no identification of students using first name and surname; first name only is to be used.
* Where services are “comment enabled”, comments are to be set to “moderated”.
* All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a license which allows for such use (i.e. creative commons).

**Notice and take down policy** – should it come to the school’s attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

**Incidents** - Any e-safety incident is to be brought to the immediate attention of the Head teacher. The e-Safety Officer will assist the Head teacher in taking the appropriate action to deal with the incident and help to fill out an incident log.

**Training and Curriculum** - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Great Moor Junior School now has planned annual programmes of training which is suitable to the audience

E-Safety for students is embedded into the curriculum; whenever COMPUTING is used in the school, staff will ensure that there are positive messages about the safe and responsible use of technology and risks as part of the student’s learning via a planned and progressive E-safety/PSHE lessons.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area, this must be brought to the attention of the Head teacher for further CPD.

**Handling E-safety incidents and complaints -** Incidents of Internet misuse will be dealt with by a senior member of staff. Any incident will follow the referral process below.

#### Flowchart for referral process for any E-safety incident or illegal activity

E-Safety Incident

Unsuitable materials

Inappropriate Activity

Report to e-safety officer and/ or head

Member of Staff

Pupil

Child Protection Issue -No

Child Protection Issue -Yes

Child Protection Issue -No

Child Protection Issue -Yes

If staff: review incident and decide on appropriate course of action, applying sanctions as necessary. Advise they get appropriate support

If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary.

Sanctions.

Inform parents

Consider:

Inform parents

Risk assess

Counselling

Discipline

Referral

Report to Head teacher and Child Protection Officer

Report to Head teacher

Report to Head teacher and Child Protection Officer

Debrief

Debrief

Review policies and technical tools

Review policies and technical tools

Implement changes

Implement changes

Monitor

Monitor

Illegal Activity

Pupil

Member of Staff

Yes a child protection issue

Not a child protection issue

Report to Police

Report to safeguarding

Secure evidence in Locked storage

Report to parents

Report to Police

Report to safeguarding

Report to Police

Report to safeguarding

Debrief

Review policies and technical tools

Implement changes

Monitor

**Important**

**Note: NEVER investigate**

 **NEVER show to others for your own assurance**

 **DO NOT let others handle evidence – Police only**

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

|  |  |
| --- | --- |
| Has the school an e-Safety Policy that complies with Child Youth Protection and Development CYPD guidance?  | **Y/N** |
| Date of latest update: |
| The Policy was agreed by governors on: |
| The Policy is available for staff at:  |
| And for parents at: |
| The designated Child Protection Teacher/Officer is:  |
| The e-Safety officer/Coordinator is:  |
| Has e-safety training been provided for both pupils and staff? | **Y/N** |
| Is the CEOP Think U Know training being considered?  | **Y/N** |
| Do all staff sign a COMPUTING Acceptable Use Policy or Code of Conduct on appointment?  | **Y/N** |
| Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?  | **Y/N** |
| Have school e-Safety Rules been set for pupils?  | **Y/N** |
| Are these Rules displayed in all rooms with computers? | **Y/N** |
| Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.  | **Y/N** |
| Has the school filtering policy been approved by SMT?  | **Y/N** |
| Is personal data collected, stored and used according to the principles of GPDR?  | **Y/N** |

#### Rules for Pupils’ Acceptable Use Policy

#### The school has installed computers and Internet access to help our learning.

#### These rules will keep everyone safe and help us be fair to others.

* **I will use only my own login and password.**
* **I will not access other people's files.**
* **I will use the computers and tablets only for schoolwork, homework and any other approved work.**
* **I will not bring USB pen drives into school without permission.**
* **I will ask permission from a member of staff before using the Internet;**
* **I will only e-mail or message people I know, or my teacher has approved;**
* **The messages I send will be polite and sensible;**
* **I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;**
* **To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive a message I do not like;**
* **I understand that the school can check my computer files and the Internet sites I visit.**
* **I will not add toolbars or download software on to my computer.**
* **If I do not follow these rules, I may be stopped from using computer technology in school**
* **I will report any concerns that I have about anything online that worries me**

GREAT MOOR JUNIOR SCHOOL

Telephone: 0161 483 4987 Southwood Road

Fax: 0161 292 3949 Great Moor

e-mail: headteacher@greatmoor-jun.stockport.sch.uk Stockport

 Cheshire

Headteacher: Kate Bushaway SK2 7DG

Dear Parents

**Responsible Internet Use**

As part of your child’s curriculum and the development of Computing and ICT skills, Great Moor Junior School provides supervised access to the Internet. We believe that the effective use of the World Wide Web is worthwhile and is an essential skill for children as they grow up in the modern world.

Although there are concerns about pupils having access to undesirable materials, we have taken strong positive steps to reduce this risk in school. Primarily, our school operates a filtering system that restricts access to inappropriate material.

Whilst we try to ensure that suitable restrictions are placed on the ability of children to access inappropriate material, the school cannot be held responsible for the nature or content of material accessed through the Internet. The school will not be liable for any damages arising from your child’s use of the Internet facilities.

Please could you and your child sign the permission slips overleaf.

Yours faithfully

K Bushaway

Headteacher

# Great Moor Junior School Consent Form

|  |
| --- |
| Please complete, sign and return to school |
| **Name of Pupil:**  |  |
| **Pupil’s Agreement**I agree to comply with the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.  |
| **Signed:**  | **Date:**  |
| **Parent’s Consent for Internet Access**I give permission for my child to use the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate material. I understand that the school cannot be held responsible for the nature or content of material accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. |
| **Signed:**  | **Date:**  |
| **Please print name:**  |

**Please answer the following two questions:**

Do you have a computer at home? Yes/No

Does your child have a tablet computer? Yes/No

Does your child have access to the internet at home? Yes/No

**Staff Code of Conduct for Network and Internet Use**

**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 e-Safety 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 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 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 e-safety policy
* I will ensure that any electronic communications with students are compatible with my professional role.
* I will promote e-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 pupils, school or school staff in relation to work on any social media sites.
* I will not have pupils as friends on social media.
* I will not use my personal mobile phone during lesson times, when pupils are present or in meetings. It will be switched off unless special permission has been given.
* I will not take photographs of pupils with any personal devices.

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

Signed: ………………………………………… Printed: ………………………………………………… Date: ……………

Accepted for use in GMJS: …………………………….……. Capitals: ………………………………...…