Great Wood Primary School
On-Line Safety Policy

Introduction

This policy applies to all members of the Great Wood community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Great Wood's digital technology systems, both in and out of the school.

This Policy is to be read alongside our:

- Pupil IT Acceptable Use Agreement
- Staff and Volunteer IT Acceptable Use Agreement
- Home School Agreement
- Mobile Phone and Camera Use Policy
- Safeguarding Policy and associated documents e.g. Keeping Children Safe in Education; Guidance for Safer Working Practice for adults who work with CYP.
- Computing and PSCHE Curriculum overviews and content
- Ed-IT Solutions SLA
- Anti-Bullying Policy
- Behaviour Policy

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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 safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the PSHCE and Computing Subject Leaders
- attendance at Online Safety training
- knowledge of the schools filtering and awareness of incidents

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead (DHT).
- The Headteacher and DHT is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead (DHT) and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those who carry out internal online safety monitoring.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead (DHT).

On-Line Safety Lead

The designated Online Safety Lead, at Great Wood, is the DHT (Miss Nicola Dixon)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- reviews the curriculum to ensure statutory Online Safety learning is mapped out across school; ensuring coverage of age- appropriate material is being taught.
- provides training and advice for staff
- liaises with the Local Authority and the technical support staff
- receives reports of online safety incidents
- reports to the Headteacher and the Online Safety Governor regularly.

Technical Support Staff

Great Wood has a Service Level Agreement with Ed-IT Solutions for internet service provision and technical support. The SLA and the scope of the filtering and monitoring service can be viewed on their website https://www.ed-itsolutions.com/ They are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher, Senior Leaders and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the Great Wood's online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement
- they report any suspected misuse or problem to the Headteacher or DHT for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- staff monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Leads
are trained in online safety issues and are aware of the potential for serious safeguarding concerns 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
- online-bullying

Pupils

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- understand research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- where appropriate will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should 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

Parents
Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- use of social media related to school
- use of on-line services related to the school – email / surveys/ on-line events such as parent/teacher meetings
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Community Users
Visitors who are given access to the school network or technology as part of wider school provisions agree the Visitors' IT Acceptable Use Agreement when they sign in at school. The Agreement can be found on our website.

The Purpose of Online Safety at Great Wood
The requirement to ensure that children are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work at Great Wood are bound. Through our Online Safety Curriculum and procedures, we

work hard to meet our statutory obligations to ensure that ALL children are safe and protected from potential harm, both within school and outside school.

In addition to key learning set out by the **National Curriculum 2014** for Computing, Great Wood Primary School ensures children are being taught the statutory learning from the **DFE's RSE document** and learning set out in the **UK Council for Internet Safety Document**, Education for a Connected World. All learning about Online Safety aims to address KCSIE 2021 Four Areas of Risk: **Content, Contact, Conduct, Commerce**.

Education- Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety/digital literacy is therefore an essential part of the Great Wood's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum provided as part of Computing/PHSCE/other lessons with key messages regularly revisited
- Pupils taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit. (All devices in school are monitored and inappropriate searches trigger notifications)
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, Facebook
- High profile events/campaigns e.g. Safer Internet Day

- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers (see appendix for further links/resources)

Education & Training – Staff and Volunteers
It is essential that all staff understand their online safety responsibilities as outlined in this policy.

- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (DHT) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff
- The Online Safety Lead (DHT) will provide advice/guidance/training to individuals as required.

Training – Governors
Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school/academy training/information sessions for staff or parents

IT Infrastructure/Equipment; Filtering/Monitoring

The school is responsible for ensuring that the school network and equipment is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

Great Wood School contracts Ed-IT Solutions to manage on-line services including filtering. Filtering is achieved through partners at EXA and their SurfProtect Filtering for Education. Current detailed information about these and a downloadable guide explaining how UK Safer Internet Centre guidance on appropriate monitoring is met through this service is available at https://www.ed-itsolutions.com/school-isp-services

The school meets recommended technical requirements:

- Regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling securely located and physical access restricted
- Clearly defined suer access rights to school technical systems and devices.
- Users with individual data (from Y2) are provided with a username and secure password by the technician who has a record of users and their usernames. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school systems, used by the technician are available to the Headteacher and kept in a secure place
- Supported by the technician, the bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring ensures that children are safe from terrorist and extremist material when accessing the internet.

- The school has provided enhanced/differentiated user-level filtering – children or adults.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- Users report any actual/potential technical incident/security breach to their teacher/the On-Line Safety Lead, the headteacher or the technician depending on level of risk
- Appropriate security measures are in place (schools may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- Visiting teachers or visitors are given access to the school network only after agreeing to the IT User Agreement when signing in and/or during induction.
- School owned devices can only be used out of school by assigned pupils and in line with the Pupil IT User Agreement.
- The Staff and Visitors' IT User Agreement prevents downloading executable files and installing programmes on school devices. The use of removable media (e.g. memory cards) is to avoided whenever possible.

Mobile Devices

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that has the capability of utilising the school's wireless network. The device then has access to the wider internet which can include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. There is a Great Wood Use of Mobile Phone and Camera Policy which outlines their use and is consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage.

The parents of pupils in Year 4 and above who walk to and/or from school alone may seek permission for their child to have a mobile phone to aid their safety out of school. There is a Pupil Mobile Phone Use Agreement which outlines the rules for pupils; these include that the phone is held by the school office during the school day. Mobile phones belonging to a child found in school during the day are confiscated.

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	-	-	-	*No*	*Yes*	*Yes*

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- The Home School Agreement enables parents to give written permission for photographs of pupils to be published on the school website/social media/local press
- The Use of Mobile Phone and Camera Policy allows parents to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims and must follow the Use of Mobile Phone and Camera Policy
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

Data Protection

Personal data will be recorded, processed, transferred and made available according to current data protection legislation.

- The Great Wood Confidentiality Policy which includes Data Protection
- Great Wood pays the Information Commissioner's Office (ICO) fee
- The bursar is the Data Protection Officer (DPO) and has a high level of understanding of data protection law and is free from any conflict of interest.

Staff:

- know to take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- ensure that they are properly "logged-off" at the end of any session in which they are using personal data

Social Media

School can be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

For the official school social media accounts

- Staff using the school social media must adhere to IT User Agreement
- Abuse and misuse is reported to the headteacher
- The school's use of our social media for professional purposes is checked regularly

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Turn off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school/academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school/academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school/academy permits reasonable and appropriate access to private social media sites.

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school/academy logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Parents

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage through the use of SurfProtect Quantum which:

- Filters digital content, within the building or on school owned devices, preventing access to the most commonly-blocked web categories and covers the types of content and communication as advised by the UK Safer Centre in the categories: Illegal, Bullying, CSE, Discrimination, Substance Abuse, Extremism, Pornography, Self Harm, Violence, Suicide;
- enables the identification of the user or device searching for banned content;
- ensures compliance with the Prevent duty;
- is updated regularly;
- is used to provide a weekly 'suspicious search' report to the IT technician- who shares concerns with the DSL.

Reviewed Summer Term 2022

Approved by Governors