Woodlands Primary School

ONLINE SAFETY POLICY

Status:	Current	
Date Adopted by Governing body:	September 2021	
Ratified by Governing Body:	20th October 2021	
Created by Matthew Kitley	September 2021	
Review by Governing Body:	October 2023	2 years

ONLINE SAFETY POLICY

This policy should be read and understood in conjunction with the following documents:

- Home School Agreement
- Behaviour Policy
- Anti-bullying Policy
- Child Protection Policy
- Guidance for Safer Working Practice for Adults working with Children and Young People
- Keeping Children Safe in Education
- Screening, Searching and Confiscation at schools (DfE 2016)
- Secure Data Handling and Record Management Policy
- Social Media and Networking Policy
- Staff Behaviour Policy
- Staff Code of Conduct

This policy has been developed by the head teacher and the computing lead and has been reviewed by the school governors.

SCOPE OF THE POLICY:

- This policy applies to all members of the school community (including: staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school's ICT systems, both in and out of the school.
- The Education and Inspections Act 2006 empowers head teachers 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 cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but are 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.
- The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies. The school will, where known, inform parents/carers of incidents of inappropriate online behaviour that takes place out of school.

ROLES AND RESPONSIBILITIES

In addition to the roles and responsibilities outlined below, and to support the implementation of this policy, the school has compiled 'Acceptable User Policies', which provide clear guidance in relevant areas such as conduct, access and use of the school system, removable media, downloading files, sharing information, social networks and devices (both school and personal equipment within and outside school.

Separate policies have been written for:

- staff (which forms part of their Code of Conduct)
- pupils and parents/carers (in the Home School Agreement)

All relevant individuals are expected to read and sign to acknowledge their responsibilities in this area. We also ask that parents/carers help to support the school in ensuring that their children understand their responsibilities and roles in online safety.

School Governors:

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the full governing body receiving termly information about online safety incidents and monitoring reports. The online safety governor will:

- have termly meetings with the online safety coordinator
- regularly monitor the online safety incident log
- report to relevant governors in and outside of governors' meeting, as necessary

Head Teacher and Senior Leaders:

- The head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The head teacher and SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The head teacher and SLT are responsible for ensuring that the online safety coordinator 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 head teacher and SLT, alongside the online safety coordinator, will ensure they collectively review any actions/ incidents that occur immediately after to offer support and guidance with actions that they have decided to put in place.

Online Safety Coordinator:

The online safety coordinator is responsible for:

- the day-to-day online safety policies and procedures
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- liaising with the Local Authority as necessary (this may be passed to the head teacher or SLT if deemed appropriate in specific instances).
- liaising with the school's technical support and external providers (Oakford)
- logging online safety incidents to inform practice, policy review and development
- meeting termly with the online safety governor to discuss current issues and review incident log
- report any incidents to the SLT

Network Manager/Technical Staff

The school's technical support (Oakford) is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements and any external guidance (i.e. DfE/Local Authority) that may apply
- users may only access the school networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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
- the use of the network, internet, learning platforms (such as Google Classroom), remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the head teacher for investigation

Teaching and support staff:

All teaching and support staff have a role to play and are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the school's current online safety policy and procedures
- they have read, understood and signed the Code of Conduct
- they report any suspected misuse or problem to the online safety coordinator or head teacher
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other

school activities (where allowed)

Designated Safeguarding Lead (DSL):

The DSL should be trained in online safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal and inappropriate materials
- inappropriate on-line contact with adults and strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

All pupils are responsible at the own level for:

- using the school's digital technology systems in accordance with the Home School Agreement
- knowing and understanding the school's rules on the use of mobile devices and digital cameras including the taking of and use of images and on cyber-bullying
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and for knowing how to do so
- understanding the importance of adopting good online safety practice when using digital technologies out of school and realising that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use internet and mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through:

- parents' evenings
- newsletters and letters
- the school's website and Learning Platform
- information about national and local online safety campaigns

Parents/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
- access to parents' sections of the website / Learning Platform and on-line pupil records
- their children's personal devices in the school (where this is allowed)

EDUCATION AND TRAINING

Staff and volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Staff and governors will be given time to read through the online safety policy and staff will be trained in the use of the online safety incident log.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and Code of Conduct.
- The online safety coordinator 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 in staff/team meetings and/or INSET days as required.
- The online safety coordinator will provide advice, guidance and training to individuals as required.

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 is therefore an essential part of the school's online safety provision.

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.
- The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
    - a planned online safety curriculum should be provided as part of computing, PHSE (and other lessons as appropriate) and should be regularly revisited
    - key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
    - pupils should be taught about online safety issues such as the risks attached to the sharing of personal details
    - pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information at an age appropriate level
    - pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet at an age-appropriate level
    - pupils should be 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 should be helped to understand the need for the Home School Agreement and encouraged to adopt safe and responsible use both within and outside school
    - staff should act as good role models in their use of digital technologies the internet and mobile devices
    - in lessons where internet use is pre-planned, it is best practice that 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 should be vigilant in monitoring the content of the websites the young people visit
    - It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that filters can be temporarily removed from those sites for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Parents/carers

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 and regulation of the children's on-line behaviours. They 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 and website
- publicising high profile events and campaigns e.g. Safer Internet Day
- reference to relevant web sites and publications.

Governors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology and online safety, health and safety and safeguarding. This may be offered in a number of ways, including participation in: school training and information sessions for staff or parents; relevant assemblies.

TECHNICAL INFRASTRUCTURE, FILTERING AND MONTIORING

Technical infrastructure and security

The school is responsible for ensuring that the school's infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. If these services are provided by an external ICT service, the school is still responsible for ensuring that the external provider fully complies with all the school's policies, procedures and acceptable user agreements as well as any Local Authority and national guidance.

- The school's technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- The school must ensure that all staff, in whatever capacity, will be effective in carrying out their online safety responsibilities.
- All users will have clearly defined access rights to the school's technical systems and devices.
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Filtering and monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content.

Internet access must be appropriate for all members of the school community from the youngest pupils to staff. 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. Neither the school nor Wiltshire Council can accept liability for the material accessed or any consequence of the internet access.

In addition to the steps already outlined above (see section on the responsibilities of the Network Manager) the school will take the following steps with regard to filtering and monitoring:

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- An appropriate system is in place for users to report any actual or potential technical incident and/or security breach to the relevant person(s), eg the online safety coordinator or the head teacher.
- Pupils will be made aware of the importance of filtering systems through the online safety

education programme
- Staff users will be made aware of the filtering systems through induction training, staff meetings, briefings and/or inset.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the internet service provider via the online safety coordinator.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. head teacher, LADO, police, Internet Watch Foundation.
- The use of computer systems without permission or for inappropriate purposes could constitute and offence under The Computer Misuse Act, 1990.

COMMUNICATION AND CONTENT

Website content
- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Where audio and video are included (e.g. Podcasts and video blogging) the nature of the items uploaded will not include content that allows the children to be identified.

Online Learning Platforms – Google Classroom
- All users will be required to use an age-appropriate password to access the relevant content of the online learning platform which must not be shared with others.
- SLT and staff will regularly monitor the usage of the online learning platform by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the online learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the online learning platform.
- All users will be mindful of individual and intellectual property and will upload only appropriate content to the online learning platform.
- When a user leaves the school, their account or rights to relevant content areas will be disabled.

Mobile Technologies
- Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.
- Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.
- Year 5 and 6 pupils may bring their mobile phones into school at the discretion of their parents/carers. However, they must be switched off and handed in to their teacher at the start of the day and collected once school has finished.

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 cyberbullying 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. 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 should inform and educate pupils about the risks associated with the taking, using, sharing, publishing and distributing of images. In particular they should recognise the risks attached to publishing their own images on the internet.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy, and in some cases protection, these images should not be published or made publically 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, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school and also ensure that when images are published that pupils cannot be identified by the use of their names.
- Photographs published on the school website, or elsewhere, that include pupils will be carefully selected and will comply with good practice guidance on the use of such images.
- 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 into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupil's work can only be published with the permission of the pupil and parents/carers.

Communications:

- The official school email service may be regarded as safe and secure and is monitored. All users should be aware that email communications are monitored.
- Users must immediately report to the DSL, in accordance with the school's policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communications.
- Any digital communication between staff and pupils or their parents/carers (email, social media, chat, blogs, Google Classroom, etc) must be professional in tone and content.

Online communication and social media:

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

Staff:

Please refer to the school's Social Media and Networking Policy for detailed guidance regarding staff use of online communications as well as the Data Protection and Secure Data Handling Policy regarding the secure handling of data and communication between agencies.

Pupils

- Pupils will be advised on security and privacy online and will be encouraged to set and regularly change passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Users must not reveal personal details of themselves or others in online communication,

including the tagging of photos or video, or to arrange to meet anyone.

- Pupils must immediately tell a responsible adult (class teacher or TA) if they receive offensive online messages.
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the SLT before using social media tools in the classroom.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites.

Video Conferencing

Video conferencing (including Skype, Teams, Google Meet) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- Staff must refer to the school's Social Media and Networking Policy and Staff Behaviour Policy/Code of Conduct prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised at all times.

Emerging Technologies

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

Cyber Bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff, parents/carers understand: how cyber bullying is different from other forms of bullying; how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and child protection policies, which include:

- Clear procedures set out to investigate incidents or allegations of cyber bullying.
- Clear procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the internet service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's online safety ethos.

Data Protection

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and any subsequent legislation.

Handling of complaints:

- The school's complaints policy and procedures can be found on the school website or alternatively a hard copy can be provided on request at the school office.
- Parents/carers and pupils will need to work in partnership with the school to resolve issues.
- Where complaints do not involve acts which are clearly illegal (e.g. accessing child abuse images or distributing racist material), they should be dealt with through the school's normal complaints procedures.
- Complaints regarding illegal activity would be dealt with in line with the school's safeguarding and disciplinary procedures and where required, would involve contact with the police and could lead to criminal prosecution, as could clear cases of cyber bullying.
- As detailed above, there are clear procedures in place to deal with concerns around cyber bullying and such incidences should be brought to the attention of the school as early as possible.
- Any complaint about staff misuse of technology must be referred to the head teacher.
- Any complaint about the head teacher should be referred to the chair of governors.
- Where any member of the school community has breached the terms of the Code of Conduct or in online safety policy, the school reserves the right to restrict their access to the school's internet.

Policy review:

This policy will be reviewed every two years, or earlier if a change in legislation or technological developments warrant it.