WOODLANDS PRIMARY SCHOOL

ONLINE SAFETY POLICY

Updated: October 2022

Review Date: October 2023

ONLINE SAFETY POLICY

Background

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school Online Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- *Access to illegal, harmful or inappropriate images or other content*
- *Unauthorised access to/loss of/sharing of personal information*
- *The risk of being subject to grooming by those with whom they make contact on the internet (CSE & Prevent)*
- *The sharing/distribution of personal images without an individual's consent or knowledge*
- *Inappropriate communication with others, including strangers*
- *Cyber-bullying / Mobile Phone bullying*
- *Access to unsuitable video and internet games*
- *An inability to evaluate the quality, accuracy and relevance of information on the internet*
- *Plagiarism and copyright infringement*
- *Illegal downloading of music or video files*
- *The potential for excessive use which may impact on the social and emotional development* and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety policy is used in conjunction with other school policies (eg Behaviour, Anti-Bullying, Acceptable Use, Safeguarding policies and Twitter policy).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to

the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development

This Online Safety policy has been developed by a working group made up of:

- *School Computing Lead*
- *Headteacher and Senior Leaders*
- *Teachers*
- *Support Staff*
- *ICT Technical staff*
- *Governors*
- *Parents and Carers*
- *Community users*

Consultation with the whole school community has taken place through the following:

- *Staff meetings*
- *Pupil Parliament*
- *Parent Forum*
- *Governors meeting*
- *Parents' evening*
- *School website and newsletters*

The school will monitor the impact of the policy using:

- *Logs of reported incidents via CPOMs (using online safety category)*
- *Internal monitoring data for network activity*
- *Pupil, parent and staff surveys – Online Safety Day*

Scope of the policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems/wifi connection, both in and out of school.

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 cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governing Body:

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 Governors receiving regular information about online safety incidents and monitoring reports. 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 Computing Lead
- Regular monitoring of online safety incident logs
- Reporting to relevant Governors'meetings

Headteacher and SLT:

- The Headteacher is responsible 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 Computing Lead.
- The Headteacher is responsible for ensuring that the Computing Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive termly monitoring reports from the Computing Lead.
- The Headteacher and another member of the Senior Leadership Team 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.

Computing Lead will:

- Lead the online safety committee (consisting of Computing Lead, Safeguarding Lead, Online Safety Governor)
- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school Online Safety policies

- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provide training and advice for staff
- Liaise with the Local Authority
- Liaise with school ICT technical staff
- Be aware of any online safety concerns that have been reported to the Safeguarding Lead, Deputy Safegurading lead, Headteacher and Deputy Head and kept on record. Incidents will inform future online safety developments
- Meet regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering
- Report to Governors
- Report termly to Senior Leadership Team

ICT Technician:

As well as an ICT Lead, the school has a managed ICT service provided by Cheshire West and Chester

The ICT Technician and Computing Lead are both responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online Safety policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- 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

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Agreement (AUP)
- They report any suspected misuse or problem to the Computing Lead and the Deputy Headteacher/Safeguarding Lead for investigation via CPOMs.
- Digital communications with pupils should be on a professional level
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school online safety and acceptable use policy

- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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

Safeguarding Lead:

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

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which parents will be expected to sign before being given access to school systems.
- Have a good understanding of 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
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking of images and on cyber-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.

Parents and Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and/or mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and website.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website in accordance with the relevant school Acceptable Use Policy.

Community Users:

Community Users who access school ICT systems and/or websites part of the Extended School provision will be expected to sign a Staff User AUP before being provided with access to school systems.

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 is therefore an essential part of the school'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 education will be provided in the following ways:

- A planned online safety programme is provided as part of Computing, SMSC and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities including Internet Safety Day
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education - Parents and 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 of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. `There is a generational digital divide`. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, social media and the school website

- Parents evenings if required

Education - Staff Training

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

- All new staff should receive Safeguarding training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies
- The Computing Lead will receive regular updates through attendance at training sessions
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings and/or INSET days
- The Computing Lead will provide advice and guidance as required to individuals as required

Training - Governors

Governors should take part in online safety training sessions, with particular importance for those who are members of any sub-committee involved in ICT, online safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority and National Governors Association
- Participation in school training sessions for staff or parents

Technical - Equipment Filtering and Monitoring

The Computing Lead will liaise with ICT Technician to ensure that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. They will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable Use Policy
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

- The school maintains and supports the managed filtering service
- Any filtering issues should be reported immediately to the ICT Technician/Computing Lead
- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Computing Lead
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Actual and/or potential online safety incident to be reported to the Computing Lead and Safeguarding Officer
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- The Staff User Agreement Policy is also in place for the provision of temporary access of `guests` (trainee teachers, visitors) onto the school system
- The Staff User Agreement Policy outlines details regarding the use of removable media (memory sticks/CDs/DVDs) by users on school portable devices
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secure

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- 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. *A list of approved websites should be provided by the class teacher for the children to access.*
- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are

many reported incidents of employers carrying 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 should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet
- Staff are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment; the personal equipment of staff should not be used for such purposes – only in exceptional cases should personal equipment be used and staff are made aware that they will be challenged when using personal equipment
- Care should be taken when taking digital and 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
- Photographs published on the website, Twitter or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media.
- Pupil's work can only be published with the permission of the pupil and parents or carers

Data Protection/GDPR

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR 2018), which states that personal data must be:

- Processed Fairly, Lawfully and Transparently
- Processed for a Specified and Legitimate Purpose
- Adequate, Relevant and limited to what is relevant
- Accurate and up to date
- Kept no longer than necessary
- Stored securely using technical and organisational measures

Staff must ensure that:

- Digital data is coded, encrypted or password-protected, both on the local hard drive and on a network drive that is regularly backed up off-site
- All electronic devices are password-protected to protect the information on the device in case of theft

- Where possible, the school will enable electronic devices to allow the remote blocking or deletion of data in case of theft
- All staff will be provided with their own secure login and password and every computer regularly prompts users to change their password
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipients
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients
- Before sharing data, staff will ensure they are allowed to share it, that adequate security is in place to share it and that who will receive the data has been outlined in a privacy notice

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- Memory sticks will not be used to hold personal information, unless they are password-protected and fully encrypted
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, eg. Keeping devices under lock and key

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and parents or carers (email) must be professional in tone and content.These communications may only take place on official school systems. Personal email addresses, text messaging or public chat and social networking programmes must not be used for these communications

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Unsuitable and Inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by CWAC and the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	

Revealing or publicising confidential or proprietary information (financial/ personal information, databases, computer access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet				✓	
Online gaming (educational)		✓			
Online gaming (non educational)				✓	
Online gambling				✓	
Online shopping				✓	
File sharing			✓		
Use of social networking sites			✓		
Use of video broadcasting e.g. YouTube			✓		

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity. For example:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.

Safeguarding pupils/students who are victims of Peer on Peer abuse

There is no clear definition of what peer on peer abuse entails. However, it can be captured in a range of different definitions:

- **Domestic Abuse**: relates to young people aged 16 and 17 who experience physical, emotional, sexual and / or financial abuse, and coercive control in their intimate relationships;
- **Child Sexual Exploitation**: captures young people aged under-18 who are sexually abused in the context of exploitative relationships, contexts and situations by a person of any age - including another young person;
- **Harmful Sexual Behaviour**: refers to any young person, under the age of 18, who demonstrates behaviour outside of their normative parameters of development (this includes, but is not exclusive to abusive behaviours);
- **Serious Youth Crime / Violence**: reference to offences (as opposed to relationships / contexts) and captures all those of the most serious in nature including murder, rape and GBH between young people under-18.

Peer on peer abuse can refer to any of the above individually or as a combination, therefore professionals working with children and young people who are experiencing abuse from their peers must respond to the needs of each of the definitions to uncover the level of complexity and respond in the most effective manner. It is possible that a young person may be sexually exploited in a gang related situation by their boyfriend or girlfriend.

Key Areas Where Peer on Peer Abuse Occurs

Bullying (including Cyberbullying)

Bullying is defined as “behaviour by an individual or group, usually repeated over time, which intentionally hurts another individual or group either physically or emotionally”. Bullying often starts with trivial events and it is behaviour that hurts someone else - such as name calling, hitting, pushing, spreading hurtful and untruthful rumours, threatening or undermining someone; mocking; making offensive comments; taking belongings; inappropriate touching; producing offensive graffiti; or always leaving someone out of groups. It can happen anywhere - at school, at home or online. It’s usually repeated over a long period of time and can hurt a child both physically and emotionally. A child that is being bullied can feel like there’s no escape because it can happen wherever they are, at any time of day or night.

There are many different forms of bullying:

- **‘Cyberbullying’**: involves sending inappropriate or hurtful text messages, emails or instant messages, posting malicious material online (e.g. on social networking websites) or sending or posting offensive or degrading images and videos;
- **Racist and Religious Bullying**: A range of hurtful behaviour, both physical and psychological, that makes a person feel unwelcome, marginalised, excluded, powerless or worthless because of their colour, ethnicity, culture, faith community, national origin or national status;
- **Sexual, Sexist and Transphobic Bullying**: includes any behaviour, whether physical or nonphysical, where sexuality is used as a weapon by boys or girls;
- **Homophobic Bullying**: targets someone because of their sexual orientation (or perceived sexual orientation);

- **Disablist Bullying**: targets a young person solely based on their disability, this can include manipulative bullying where a perpetrator forces the victim to act in a certain way, or exploiting a certain aspect of the victims disability.

It is important to remember that bullying can also be a combination of the above. There has been much media attention surrounding children and young people who have committed suicide due to being bullied. Professionals must understand the damaging and at times fatal effects bullying can and does have on children and young people and be able to respond to it effectively

Safeguarding pupils/students who are victims of the sharing of nudes or semi-nude images/videos

Whilst professionals refer to the issue as 'sexting' there is no clear definition of 'sexting'. Many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet.' Yet when young people are asked 'What does sexting mean to you?' they are more likely to interpret sexting as 'writing and sharing explicit messages with people they know'. Similarly, many parents think of sexting as flirty or sexual text messages rather than images.
This only covers the sharing of sexual imagery by young people. Creating and sharing sexual photos and videos of under-18s is illegal and therefore causes the greatest complexity for schools and other agencies when responding. It also presents a range of risks which need careful management.
On this basis current advice introduces the phrase 'youth produced sexual imagery' and uses this instead of 'sexting.' This is to ensure clarity about the issues current advice addresses.

'Youth produced sexual imagery' best describes the practice because:

- 'Youth produced' includes young people sharing images that they, or another young person, have created of themselves.
- 'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context.
- 'Imagery' covers both still photos and moving videos (and this is what is meant by reference to imagery throughout the document).

The types of incidents which this covers are:

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18

For the best way to respond to these issues, staff should read the following advice:
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

WOODLANDS PRIMARY SCHOOL

Staff (and Volunteer) Acceptable Use Policy

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 communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Scope

This policy covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, for example:

- email systems (internal and external)
- internet and intranet (email, web access and video conferencing)
- telephones (hard wired and mobile)
- computers – *this covers ANY computer used for work purposes, whether at the place of work or elsewhere*
- iPads and other tablet devices – *this covers ANY tablet device used for work purposes, whether at the place of work or elsewhere*
- photocopying, printing and reproduction equipment
- documents and publications (any type or format)

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, websites etc.) out of school.
- I understand that the school ICT systems are intended for educational use and that I will only use the systems for personal or recreational use within the policies (Online safety, Safeguarding, Staff Handbook and ICT policy) and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person (a member of the SLT) and record in the log book in each ICT room.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others (including children) I will do so with their permission and in accordance with the school's policy on the use of digital / video images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. I will not mention Woodlands Primary School on social media in a negative or inappropriate manner.
- I am allowed to take digital and 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;only in exceptional cases should my personal equipment be used and I am aware that I will be challenged when using personal equipment
- I will use social networking sites in school in accordance with the school's policies (Onlin Safety, Safeguarding, Staff Handbook and ICT policy).
- I will adhere to the school online safety, Staff Handbook and safeguarding policies at all times.

I will only communicate with students / pupils and parents / carers using official school systems and email addresses. Any such communication will be professional in tone and manner. There will be no communication with parents/families using personal email addresses or telephones:

- No details of pupils will be stored on laptops or taken out of school unless on a visit/trip and they will be kept by the group leader confidentially.
- Photographs of children will be taken on school equipment; only in exceptional circumsatnces will photos be taken on personal phones or cameras and they will not be stored on laptops unless on a school residential. They must be deleted once transferred in school to the school ICT system and this must be observed by a member of the SLT.
- I will not use my mobile phone whilst children are present and will ensure that it is locked away in a store cupboard. I will not charge my mobile phone in a classroom.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and CWaC local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

When I use my personal hand held / external devices (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 school equipment. 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. Mobile phones will only be used in the PPA room or the staff room during break/lunchtimes or with the consent of the Head teacher or a senior member of staff.

- I will not use personal email addresses or access personal networking sites on the ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- If I wish to install a programme onto equipment that is owned by school, I will contact the computing lead first.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. If equipment is damaged, I will report it to school immediately

and be aware I may be responsible for the cost of repair if not covered by our school insurance.

- I understand that data protection policy requires that any staff or student / pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action which may include termination of contract. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

I have read and understand the Staff/Volunteer Acceptable Use Policy

Staff / Volunteer Name …… (Print)

Signed ……

Date ……

WOODLANDS PRIMARY SCHOOL

PUPIL COMPUTING SAFE USE AGREEMENT

Dear Parents and Carers,

ICT, including the internet, e-mail and mobile phone technologies have become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these online safety rules with your child(ren), explaining the content, age-appropriate, with them.

If you have any concerns or would like some explanation please contact your child's class teacher.

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when emailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, videos, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my online safety.

ONLINE SAFETY ACCEPTABLE USE AGREEMENT

We have discussed this and ……..... (child's name) agrees to follow the online safety rules and to support the safe use of ICT at Woodlands Primary School.

Parent/ Carer Signature …….…… Date ……