WOODLANDS PRIMARY SCHOOL, HEDGEHOGS NURSERY AND SUNBEAMS CLUB (+Vistors to School)

ONLINE SAFETY POLICY

Updated: October 2025

Review Date: November 2028

Woodlands Primary School, Hedgehogs Nursery, Sunbeams Club
Staff and Visitors 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 and strong cybersecurity protections at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately, securely, and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Woodlands Primary, Hedgeshogs, Nursery and Sunbeams club (the school) Online Safety policy and cyber security incident response plan (see separate document) should help to ensure safe, secure, 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 Senior Leaders, 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 (data breaches, identity theft, cyber attack)
• 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
• Cybersecurity threats such as hacking, phishing, ransomware, and malware that target personal devices and school networks
• 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 offline world, but cyber security introduces additional challenges that require strong technical controls (such as firewalls, secure passwords, encryption, and monitoring systems) alongside digital literacy education. It is essential that this Online Safety and the cyber security incident response plan is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying, Acceptable Use, Safeguarding policies, Social Media Policy, cyber security incident response plan).

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, knowledge, and cyber security 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 and cyber security incident response plan 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, informed, and secure users who can 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 E-Safety or Filtering and Monitoring category)
- Internal monitoring data for network activity
- Pupil, parent and staff surveys

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/Wi-Fi 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 cyber security incident response plan and for reviewing the effectiveness of them. 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 Safety Governor.

The role of the Safety Governor will include:

- Regular meetings with the Computing Lead
- Regular monitoring of online safety incident logs

- Ensure that the leadership team and relevant staff and aware of and understand the flitering and monitoring systems that are in aplace and how to manage them effectively.
- Reporting to relevant Governors'meetings
- Ensure that they have participated in updated cyber security training.

- The Chair of Govenors is part of cyber security incident response team if an attack was to happen against the school.

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 Computing Lead will receive daily reports from an external provider (Schools Broadband, using Netsweeper) who are monitoring the computing work and online usage of staff, children and guests. In addition to this, if any online safeguarding issues happen during the day in school the Computing Lead is emailed to deal with this issue.
- The Headteacher/Senior Leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.
- 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.
- The headteacher is responsible for helping to create and follow the cyber security incident response plan if an attack was to happen against the school.

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
- Help to create, update and follow the cyber security incident response plan if an attack was to happen against the school.
- Ensure that children are being educated in online safety and cyber security.

ICT Technician:

As well as a Computer Lead, the school has a managed ICT service provided by School ICT Support LLP.

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
- That all staff are set up with Bitcodes on their laptops and two-step verification for school emails for added security
- Help to create, update and follow the cyber security incident response plan if an attack was to happen against the school.

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 discussions and activities are embedded in all aspects of the curriculum and other school activities (half termly online safety lessons, computing lessons, assemblies, visitors, internet safety days, police visits and workshops)
- Pupils understand and follow the school online safety and acceptable use policy which is talked about at the start of each school year and recapped each term. Rules are displayed in classrooms and computer suites.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor computing activity in lessons, extra-curricular and extended school activities via Classroom Cloud or Veyon
- They follow the cyber security incident response plan if an attack was to happen in school
- 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

The Safeguarding Lead should take responsibity for understanding the filtering and monitioring systems and procedures that are in place.

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
- Should follow the Acceptable Use policy and computing rules at all times, recapped each half term

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, information via Seesaw or Tapesrty (The schools communication tool for parents) and the schools website. The school will also provide parents and carers of the filtering and monitoring systems that are in place, what children are being asked to do online, including websites that they are being asked to access and who (if anyone) they will be interacting with online.

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 and Student Teachers:

Community Users, including student teachers, 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. In order for them to be able to access the schools Wi-Fi, they will be given a guest Wi-Fi password and code, this will be accessable for their length of stay within the school. Guest must agree and tick to give consent, to the following terms and conditions before being able to sign into the Wi-Fi:

- I agree to use the schools Wi-Fi for professional and educational use only.
- I agree that I will not use the schools Wi-Fi for personal use, social media use or to download inappropriate data.
- I understand that any inappropriate wording may be monitored and reported to SLT.
- The wireless network is provided "as is" without warranties of any kind, either expressed or implied.
- I agree not to use the wireless network for any purpose that is unlawful and take full responsibility of my acts.

Education and Curriculum for 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, computing lessons and wider curriculum. 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 to run alongside the computing curriculum. This is planned via Project Evolve and follows each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World". One lesson is taught per half term for each year group and follow up questions, discussion stories and awareness is embedded in the computing curriculum.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities including Internet Safety Day and visitors to the school, which include the local police for talks, workshops and 'Cyber Sid' visits.
- Children will take part in planned cyber security lessons to help them understand the need for strong passwoords, protecting their devices and suspicious content
- 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. This is shared with the children at the start of each term and displayed in classrooms
- 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
- Children's mobile phones, if they bring them to school, are handed into the class teacher at the start of each school day and given back at hometime. Children are not allowed their phones during the school day and must be switched off.

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 online 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, Seesaw and the school website
- Parents evening and police talks if required

Education - Staff Training

It is essential that all of our staff receive online safety and cyber security 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
- All staff need to have cyber security training at the start of each school year. This is an insurance requirement to ensure the school is covered in an attack. Signed proof and certificates of the training are required.
- Police visits and talks for the staff on cyber security will take place during staff meetings

Training - Governors

Governors should take part in online safety training sessions and Cyber Security training, with particular importance for those who are members of any sub-committee involved in computing, 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
- Onlline workshops and videos

Technical - Equipment Filtering and Monitoring

The Computing Lead will liaise with the 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 staff are provided with a username and password and children in Y5/6 have individual password protected Google accounts to access the Chromebooks
- 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 Via CPOMS
- 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 incidents to be reported to the Computing Lead and Safeguarding Lead Via CPOMS
- 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
- A basic monitoring system is in place within the school. This monitors the use of websites and search engines for staff, children and guests within the school. Any inappropriate language used within website searches is flagged up in a daily reprt which is sent to the Computing Lead. This is then followed up with individuals and recorded via CPOMS.
- Live monitoring can take place with the use of Classroom Cloud, to monitor Chromebooks and laptops, or Veyon, to monitor the desktops, during lessons, staff can access these monitoring programs to observe what the children are doing during computing time.

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, Seesaw 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 particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/Seesaw or used within school.
- 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

Memory sticks and removable storage are not advised within the school. However, if they are needed to be used then the following guidenlines must be followed:

- The data must be encrypted and 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
- USB sticks or portable hard drives should not be used with the school system as they might have viruses. Staff must not save sensitive or personal data on these devices unless the school has approved and encrypted them.
- If staff use USBs on their home computers, they must make sure their home computer has updated antivirus software to prevent spreading viruses to the school network.

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 Child on Child 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

Sexting occurs when people share sexual messages via text, social media or email, and/or naked or semi-naked images with another person. Children and young people may also talk about sharing 'nudes' or 'pics'.

Young people, including children, may consent to sending a nude image of themselves. They can also be forced, tricked, or persuaded into sharing these images by another. Whether a child or young person shares an image consensually or not, they have no control over how other people might use or share it.

People who are involved in a sexting may have:

- shared an image of themselves
- asked for an image from someone else
- received an unsolicited image
- shared an image of someone else

According to NSPCC, 'It's a criminal offence to create or share explicit images of a child. However, the law is intended to protect children and not criminalise them. If sexting by a young person is reported to the police, they will make a record but depending on the circumstances they may decide not to take any formal action.'

If staff become aware of children being involved in sexting, then the normal procedure for reporting this safeguarding concern should be reported via CPOMS to the DSL. This should be tagged within online safety and the Computing Lead be informed.

UK Council for Internet Safety (UKCIS), have produced guidance for school settings on sharing nudes and semi-nude. This guidance includes what to do if staff become aware that a chid has been involved in sexting and advice on how to respond to sexting.

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
For more information from NSCPP see https://learning.nspcc.org.uk/online-safety/sexting-sharing-nudes-semi-nudes

Below is the Acceptable Use Policy for staff, visitors and the children.

Woodlands Primary School, Hedgehogs Nursery and Sunbeams Club Staff and visitors Acceptable Use Policy

New technologies are now a big part of most people's lives, both in and out of school. The internet and other digital tools offer many new opportunities for learning and communication. They can help spark discussion, boost creativity, and support better learning for all. These tools also help teachers work more creatively and efficiently. It is vital to keep staff, governors, children and school visitors safe at Woodlands Primary School, Hedgehogs Nursery and Sunbeams Club (the school) as well as the schools IT systems and devices. This Acceptable Use Policy, when followed, will help to keep everyone safe as well as the schools IT systems and users protected from mistakes or misuse that could cause problems or security risks.

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)
- computing devices – *this covers ANY computing device used for work purposes, whether at the place of work, home or elsewhere*
- photocopying, printing and reproduction equipment
- documents and publications (any type or format)

Acceptable Use Policy Agreement

The school is committed to providing staff and volunteers with good access to ICT to support their work both in and out of school, and to enhance pupils' learning. In return, the school expects all staff and volunteers to use ICT responsibly by agreeing to and following the guidelines outlined below.

Computer Security and data Protection

- Every staff member will get their own school computer account with a personal username and password. This account will match the level of access they need and should not be shared.
- Passwords must be strong. Use three random words with capital letters, numbers, and symbols. Never share your password with anyone and they should not be kept near or on any computing device.
- Passwords for any school device (computers, laptops, iPads, tablets etc) should not be given to children.
- Each laptop has a Bitcode for access. Staff must not store this Bitcode on or near their laptops
- Children should not use staff accounts. If they do (which is not advised), they must be supervised and not left alone with the device. Staff are fully responsible for any problems that happen as a result.
- When leaving a computing device unattended, staff must log out or lock the screen to stop others from accessing their account or emails.
- USB sticks or portable hard drives should not be used with the school system as they might have viruses. Staff must not save sensitive or personal data on these devices unless the school has approved and encrypted them.
- If staff use USBs on their home computers, they must make sure their home computer has updated antivirus software to prevent spreading viruses to the school network.
- If staff use a personal computer or device at home for school work, they must not store any sensitive or personal school data unless the device is fully encrypted by IT support and approved by the headteacher.
- The school server and emails are backed up every night. Staff should regularly back up files from their Desktop and Downloads folder, as these may not be included.
- It is the responsibility of the staff to ensure laptops, tablets, iPads, cameras, and other school devices are locked away at the end of the day and not left where they can be seen through windows or doors.
- Do not click on links or open attachments from unknown or untrusted email sources. Report any suspicious, harmful, or inappropriate content or emails right away to IT support or the Computer Lead.

- In the event that your device is lost or stolen, you must inform the school immediately who will advise on the next steps.

Conduct

Staff must…

- Always use the school's computer system in a professional, polite, and legal way that does not harm the school's or their own reputation.
- Not access, use, download, or share illegal or harmful content, such as child abuse images, racist material, or pornography.
- Use or share offensive, rude, racist, sexist, or threatening language or material or make jokes or comments about someone's race, gender, or sexual preference.
- Follow and respect the school's computer security rules and not try to get around them.
- Not damage or harm any school computer or device.
- Not download large amounts of data or store lots of personal files on the school system.
- Not access, copy, or change another person's files without permission.
- Only contact pupils, parents, or carers using school email accounts or systems, and always be professional. These communications should be recorded on CPOMS. Personal phones or email accounts must not be used.
- Ensure that pupil information must is not stored on laptops or taken off school grounds unless for a trip, and only by the group leader which will be kept securely.
- Ask IT support or Computer Lead if they want programs installed onto computing devices.
- Keep all pupil and staff data private, unless required to share by law or school policy.
- Have permission before using someone else's work and follow copyright rules. Music, videos, and other protected materials should not be copied or shared illegally.
- Be responsible for their actions, both in and out of school.

Mobile Phones

- Staff must not use their mobile phones when children are present. Phones should be switched off or on silent and kept out of sight, such as in a cupboard or a bag, during the school day.
- Staff must not charge their phones in the classroom.
- Phones can only be used in the PPA room or staff room during breaks or lunchtime, or with permission from the Headteacher or a senior staff member.
- Children must never be allowed to use staff mobile phones.
- Staff must not use personal phones to take photos or videos of children or to update Seesaw/Tapestry unless the Headteacher has given permission. If allowed, photos must be moved to the school computer system immediately and then deleted from the phone. However, if mobile phones are the only device available and are used to take photographs they should only be used in exceptional circumstances.
- Phones are only allowed to be accessed in classrooms when needing to use two-step verification to access school emails.
- If a member of staff needs to make an urgent personal phone call they can use their phone at an appropriate non-contact time If a member of staff has a family emergency or similar and needs to keep their mobile phone to hand, prior permission must be sought from their phase leader.

Personal Use

The school allows staff to use school computers for personal reasons from time to time, as this can help improve IT skills and support a good work-life balance. This is allowed under the following conditions:

- Staff must still follow this Acceptable Use Policy and all other school rules for staff behaviour.
- Personal use must not slow down or affect the school's computer system.
- Staff laptops must not be used for business or commercial work unless the school gives permission.
- IT support monitors all computer use, whether it's for work or personal reasons. If you access private information, you do so at your own risk.

- Staff must not store personal files on the school system, including:
- Music
- Games
- Videos
- Photos or images

If these types of files are found, staff will be asked to delete them.

Photographs

- Staff must get permission before taking or sharing photos or videos of other staff or children, and must follow the school's rules on using digital images. If images are shared (e.g. on the school website), names or personal details will not be included.
- Photos shared on Seesaw or Tapestry will include a child's first name and first letter of their surname. Parents have been informed and have given permission for this.
- Staff can take photos or videos for educational purposes, but must follow school rules on how these are shared and used. Images should only be taken using school devices. In rare cases where a personal phone is used, the photos must be deleted as soon as possible.

Smartwatches

- Staff are permitted to wear smartwatches at school; however, if the device includes a camera function, it must not be used to operate the camera—either directly or via a connected mobile phone—in accordance with the above guidelines on mobile phone use

Supervision of Pupils

- Pupils must always be supervised when using school computers or mobile devices during lessons.
- Staff should regularly remind children about the Acceptable Use Policy to help keep them and the devices safe.
- Children must not use computing equipment without supervision during break or lunchtime.
- Staff can use 'School Cloud' or 'Vygon' to monitor pupils' work during lessons, and are encouraged to do so.
- All children's mobile phones must be collected at the start of the day and locked away safely. Phones are returned at the end of the school day. Children should not use them during school hours.
- Children should be informed that their computer use is being monitored. Any inappropriate internet searches will be flagged, and parents will be informed of any misuse.
- All staff should teach the children about how to use ICT and the internet safely whenever possible.
- Teacher tablets have staff access only. Children must be supervised when using these and use them at the risk of the teacher.

Use of Social Networking, Websites and Online Forums

Staff should be careful when using social media, even in their own time. Please follow these rules:

- Do not use social media during school time or on school devices.
- Do not add pupils as friends or message them privately on social media, even for school reasons.
- Be careful what you post online. Make sure your comments don't harm your professional reputation or that of the school.
- Unless you have permission, do not post anything that makes it seem like you are speaking for the school.
- Do not mention the school on social media in a negative or inappropriate way.

Use Of Your Own Equipment – Bring Your Own Device

- If you bring your own device to school, it's your responsibility. The school is not responsible for any damage or loss. When not in use, keep it in a safe place.
- Do not store school photos or videos that include staff or children on your personal devices like phones or tablets.
- Do not connect your personal devices to the school's computers or network without permission from IT Support.

Any staff member, volunteer or student found to be non-compliant with this policy will face disciplinary action.

WOODLANDS PRIMARY SCHOOL, HEDGEHOGS, NURSERY AND SUNBEAMS CLUB
PUPIL COMPUTING ACCEPTABLE USE

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 and computing 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.

EYFS and Key Stage 1

When I use the school computing equipment or go online at school, I promise to this do these things:

- Look after all the computing equipment
- Ask for help if I need it
- Only use the equipment if I have been asked by a member of staff
- Only take a picture or video of other people if they say it is ok
- Use all the equipment sensibly
- Tell an adult I know if I see something that makes me worried or unhappy
- Only search the internet for sensible things

Key Stage 2

When I use the school computing equipment or go online at school, I promise to this do these things:

- Use the schools computing equipment safely and responsibly
- Keep my passwords and personal information private and not share with others
- Report anything that I see online that upsets or worries me
- Only post polite, positive and kind comments
- Not to take photos or videos of others without their permission
- Not to search for inappropriate material online
- Use school equipment and the internet to complete work set by members of staff and not for anything else
- I will not upload any images, videos, sounds or text that could upset any member of the school community.
- I know that my computing work 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 and computing rules and to support the safe use of ICT at Woodlands Primary School, Hedgehogs, Nursery And Sunbeams Club

Parent/ Carer Signature …….. Date ……