E-Safety Policy Draft

To be ratified 20.3.24.

Responsibility for oversight and update of this policy	Headteacher and Computing Lead
Last Updated	March 2024
Review Date	March 2025

1. Aims

Our school aims to:

• Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
• Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
• Identify and support groups of pupils that are potentially at greater risk of harm online than others
• Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
• Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:
• Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
• Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
• Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
• Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam
These risks do not stand in isolation, however, and it is important to understand the interplay between them.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

• Teaching online safety in schools
• Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
• Relationships and sex education
• Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board
The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks (being careful that 'overblocking' does not lead to unreasonable restrictions), and will regularly review their effectiveness.
The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:
• Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
• Reviewing filtering and monitoring provisions at least annually;
• Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
• Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:
• Ensure that they have read and understand this policy
• Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
• Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
• Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate

for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher
The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead
Details of the school's DSL and deputy are set out in our child protection and safeguarding policy as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:
• Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
• Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
• Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
• Working with the Computing Lead to make sure the appropriate systems and processes are in place
• Working with the headteacher, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
• Managing all online safety issues and incidents in line with the school's child protection policy
• Ensuring that any online safety incidents are logged and monitored (on My Concern) and dealt with appropriately in line with this policy
• Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
• Updating and delivering staff training on online safety
• Liaising with other agencies and/or external services if necessary
• Providing regular reports on online safety in school to the headteacher and/or governing board
• Undertaking annual risk assessments that consider and reflect the risks children face
• Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEN in a college and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.
• Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Computing Lead
The Computing Lead is responsible for:
• Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
• Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
• Conducting a full security check and monitoring the school's ICT systems on a monthly basis;
• Blocking access to potentially dangerous sites and, where possible, preventing the

downloading of potentially dangerous files;
• Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
• Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
• As listed in the 'all staff' section, plus:
• Overseeing the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
• Working closely with the PSHE and Wellbeing lead to avoid overlap but ensure a complementary whole-school approach
• Working closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:
• Maintaining an understanding of this policy
• Implementing this policy consistently
• Recognising that PSHE and Wellbeing is a statutory whole-school subject requiring the support of all staff and that online safety is embedded within this subject
• Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
• Working with the DSL to ensure that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy
• Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and are recorded on My Concern
• Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
• Reading part 1, Annex B and Annex D of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections).
 • Modelling safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
• Ensuring that any websites that are planned to be used in lessons are appropriate and should teachers need a website 'unblocking', they are responsible for checking it's suitability before asking for it to be unfiltered for pupils.

This list is not intended to be exhaustive.

3.6 PSHE and Wellbeing Lead

As listed in the 'all staff' section, plus:

• Embedding consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives." This will complement the

computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

• Working closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE and Wellbeing

• Working closely with the Computing Lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

3.7 Parents / Carers
Parents are expected to:
• Notify a member of staff or the headteacher of any concerns or queries regarding this policy
• Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
• Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
Parents can seek further guidance on keeping children safe online from the following organisations and websites:
• What are the issues? – UK Safer Internet Centre
• Hot topics – Childnet International
• Parent resource sheet – Childnet International
• Healthy relationships – Disrespect Nobody

3.8 Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:
The text below is taken from the National Curriculum computing programmes of study.
It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.
All schools have to teach: Relationships education and health education in primary schools
In Key Stage 1, pupils will be taught to:
• Use technology safely and respectfully, keeping personal information private
• Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
Pupils in Key Stage 2 will be taught to:
• Use technology safely, respectfully and responsibly
• Recognise acceptable and unacceptable behaviour
• Identify a range of ways to report concerns about content and contact
By the end of primary school, pupils will know:

• That people sometimes behave differently online, including by pretending to be someone they are not
• That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
• The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
• How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
• How information and data is shared and used online
• What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
• How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
• How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
• How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online) The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. Online safety is constantly talked about in class when children are accessing the internet, for example.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during parents' evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.
6.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail on training).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices
School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
• Poses a risk to staff or pupils, and/or
• Is identified in the school rules as a banned item for which a search can be carried out, and/or
• Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
• Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL or headteacher.
• Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
• Seek the pupil's co-operation Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the device, data or file in question has been, or could be, used to:
• Cause harm, and/or
• Undermine the safe environment of the school or disrupt teaching, and/or
• Break any of the school rules
If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, headteacher or other member of the senior leadership team to decide whether they should:
• Delete that material, or
• Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
• Report it to the police*
* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element. If inappropriate material is found on the device, it is up to (the staff member in conjunction with the DSL, headteacher or other member of the senior leadership team) to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

• They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
• The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
• Not view the image
• Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next.
The DSL will make the decision Any searching of pupils will be carried out in line with:
• The DfE's latest guidance on screening, searching and confiscation
• UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Social Media

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups. If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure (see our complaints policy) should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve). Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults. Regular articles on online safety are included in our school newsletter, which support parents in understanding and tackling issues to do with online safety. Email and E-Schools are the official electronic communication channels between parents and the school and between staff and pupils.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives).

In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute. Breaches will be dealt with in line with the school behaviour and relationship policy or anti-bullying policy (for pupils) or code of conduct/handbook (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media or group post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.
Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

6.5 Upskirting
It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

6.6 Use of Artificial intelligence (AI) in cyber-bullying
Generative artificial intelligence (AI) tools are now widespread and easy to access. The Woodlands Community Primary School recognises that AI has many uses to help pupils learn (see section 7.2 below), but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, impersonation and audio or video hoaxes that look real. The Woodlands Community Primary School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour and relationship policies. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

7.1 Filtering and Monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." At The Woodlands Community Primary School, we have dedicated and secure firewalls (securus) providing multiple layers of security including a web filtering system to filter all devices on our network to ensure the websites visited by pupils, staff, volunteers, governors and visitors to the school are appropriate. The filtering system is tested regularly, but if any inappropriate material does get through, then pupils and staff should report this immediately in order to get it blocked. In planning lessons, should teachers need a website 'unblocking', they are responsible for checking its suitability before asking for it to be unfiltered for pupils.

7.2 Use of AI

In school AI should enhance, not replace, human creativity. Teachers may use AI within lesson creation (e.g. planning, quiz creation, flashcard generation, text generation), but they must verify the suitability, accuracy and curriculum alignment of any AI-generated materials. Any AI-generated content must be checked to ensure that it is accurate and factually correct. Before using any new software, it should be evaluated and reviewed by the teacher to ensure that it is fit for purpose. If in doubt, a member of SLT should be consulted.

8. Storing and Sharing Data

8.1 School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher/Principal and Governors have delegated the day-to-day responsibility of updating the content of the website to LSalt. The site is managed by / hosted by E-Schools.

The DfE has determined information which must be available on a school website. Where other staff submit information for the website, they are asked to remember:

• Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.

• Where pupil work, images or videos are published on the website, their identities are protected and full names are not published in line with parental consents, which are collected each year.

8.2 Cloud platforms

Office 365 is utilised for storing of files and data and has a 2-factor authentication access. For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush–never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. Staffs Tech analyses and documents systems and procedures before they are implemented, and regularly review them.

The following principles apply:

• Privacy statements inform parents when and what sort of data is stored where

• The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought

• Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such

• Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
• Pupil images/videos are only made public with parental permission
• Only school-approved platforms are used by students or staff to store pupil work
• All stakeholders understand the difference between consumer and education products E-Schools/School Website (EYFS-Y6) is utilised to store pupil work. Images and videos are only shared once parental permission has been obtained.
EYFS no longer uses tapestry to record learning journeys. It is not online based.

8.3 Digital Images and Video
When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.
Parents answer as follows:
● For the school newsletter
● For newspapers
● For use in paper-based school marketing
● For the school website
● For a specific high-profile image for display or publication

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them). All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At The Woodlands Community Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils whilst in school. Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos)- this will only happen on occasions such as school trips in order to share photos of events once back in school. Photos are stored on office 365 in line with the retention schedule of the school Data Protection Policy. Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children. Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information. Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

9. **Pupils using mobile devices in school**

9.1 Mobile Phones
Pupils may bring mobile devices into school, but they are handed into the class teacher for safe keeping until the end of the school day. Pupils must not turn their phones on whilst

on the school premises. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

9.2 Smart Watches
If a smart watch has camera facilities, messaging and call services and independent access to the internet, they present the same concerns as mobile phones in terms of safeguarding. Therefore, such devices should not be worn to school. If they are brought onto the premises, they should be handed to the class teacher for safe keeping until the end of the school day. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:
• Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
• Making sure the device locks if left inactive for a period of time
• Not sharing the device among family or friends
• Keeping operating systems up to date – always install the latest updates
Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from L.Leedham-Hawkes/C.Read/Entrust

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology in school, or the right to bring devices onto school property.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Training will also help staff:
- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

13.Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on My Concern. This policy will be reviewed every year by the Headteacher, Computing Lead and senior leadership team. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:
- Child protection and safeguarding policy
- Behaviour and Relationship policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- RSE policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - o I click on a website by mistake
    - o I receive messages from people I don't know
    - o I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material);
- Use them in any way which could harm the school's reputation;
- Access social networking sites or chat rooms (other than the school's Facebook page to promote or celebrate something in school);
- Use any improper language when communicating online, including in emails or other messaging services;
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network;
- Share my password with others or log in to the school's network using someone else's details;
- Take photographs of pupils without checking with teachers first or checking the consents on the One Drive;
- Share confidential information about the school, its pupils or staff, or other members of the community;
- Access, modify or share data I'm not authorised to access, modify or share;
- Promote private businesses, unless that business is directly related to the school;

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school can monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	Date: