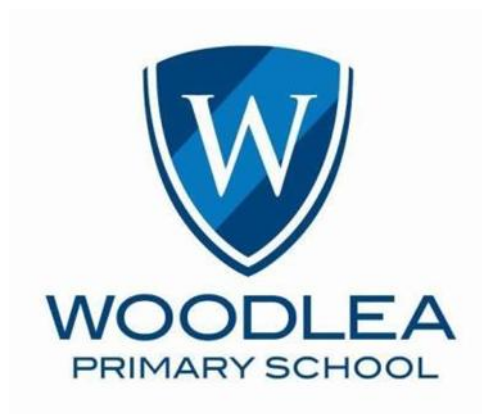




Woodlea Primary School Online Safety Policy

Reviewed by	Governors/Head Teacher
Reviewed in	Autumn 1 2026
Status & Review Cycle	Every 2 years
Next Review date	Autumn 1 2028

Contents

Employee Wellbeing	3
Public Sector Equality Duties	3
Aims	3
Legislation and guidance	3
Roles and responsibilities.....	4
The governing board	4
The headteacher	4
The designated safeguarding lead	5
The IT network manager.....	5
All staff and volunteers	5
Parents	6
Visitors and members of the community	6
Educating pupils about online safety	6
Educating parents about online safety	7
Cyber-bullying	8
Definition	8
Preventing and addressing cyber-bullying.....	8
Examining electronic devices	8
Acceptable use of the internet in school.....	10
Pupils using mobile devices in school	10
Staff using work devices outside school	10
How the school will respond to issues of misuse	11
Training	11
Monitoring arrangements	11
Links with other policies.....	12
Appendix 1: EYFS and KSI acceptable use agreement (pupils and parents/carers)	13
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers).....	14
Appendix 3: Acceptable use agreement (staff)	16
Appendix 4: Acceptable use agreement (governors, volunteers and visitors)	18
Appendix 5: Online safety training needs – self-audit for staff.....	19
Appendix 6: Online safety incident report log	20

Employee Wellbeing

Tandridge Learning Trust is committed to promoting the positive mental, physical and emotional wellbeing of its staff and recognises that enhancing individual wellbeing offers benefits not just to our staff but also to the wider communities within our organisation.

As such, when implementing this policy, consideration will be given to the impact on workload and wellbeing and take appropriate action to monitor, mitigate and support all those involved in its application.

Public Sector Equality Duties

Tandridge Learning Trust is committed to equality, both as an employer and a service provider. We welcome our general duty under the Equality Act 2010 to eliminate discrimination, to advance equality of opportunity and to foster good relations. We will ensure diligence in regard of our specific duties. This policy will be consistently and fairly applied to all stakeholders, with due regard for ensuring no-one experiences less favourable treatment in its application.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 (which we refer to as 'mobile phones')
- 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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
 - **Conduct** – 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), including those generated using AI, and online bullying; and
 - **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

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

- [Teaching online safety in schools](#)
- [Meeting digital and technology standards](#)
- [Preventing and tackling bullying](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Mobile phones in schools](#)

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](#) the [Children's Wellbeing and Schools Act 2026](#) 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.

This policy complies with our funding agreement and articles of association.

Roles and responsibilities

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 ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board, will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The Trust board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the 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 the school's safeguarding needs

The governors who oversees online safety are [Kirsty Irvine](#).

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 4](#))
- 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 special educational needs and/or disabilities (SEND). This is 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

The headteacher

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

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances – for example, a confidential shared mailbox to make sure safeguarding concerns are received, monitored and acted on without delay.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy designated safeguarding leads (DDSLs) 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 ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT network manager 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 child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged ([see appendix 6](#)) 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 ([appendix 5 contains a self-audit for staff on online safety training needs](#))
- 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
- 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.

The IT network manager (Central IT Team)

The IT network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

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

- 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](#))
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by, [informing the DSL, Office team & logging them on the IT Portal](#).
- Following the correct procedures by requesting access from Headteacher and IT Central Team through IT portal if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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
- 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'

This list is not intended to be exhaustive.

Parents

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](#))

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](#)

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 4](#)).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. See the Online Safety Curriculum Policy for the programme of study.

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary 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
- [Be discerning in evaluating digital content](#)

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites, which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with 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, and some pupils with SEND.

Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

- The school's expectations in respect of appropriate use of AI by pupils

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher (DSL) or DDSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

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. (See also the school behaviour policy.)

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 and assemblies will be used to address the subject.

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.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device in line with our search and confiscation policy which is found in our behaviour policy.

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- 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 cooperation

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 data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the headteacher(DSL) or in the absence of the headteacher, 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), **including any image generated or altered by AI, they will not:**

- View, copy, print, share, store, save, forward on, or ask a child to share or download the image
- Delete the image or ask the pupil to delete the image
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any pupil involved

The staff member will 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 in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

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 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', or "deep nudes", where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils in line with our behaviour policy.

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/trust and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

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 to 4](#)). 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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and [restrict access through filtering systems where appropriate](#).

More information is set out in the acceptable use agreements in [appendices 1 to 4](#).

Pupils using mobile devices in school

[In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones \(e.g. smart watches\), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.](#)

Only pupils in Year 6, who walk to or from school, are allowed mobile devices. [No Smartphones are allowed, only brick phones](#). Permission must be sought and an agreement signed. These are not permitted to be used on school premises or when attending activities organised by the school.

[Any deviation from this mobile phone-free baseline will be by exception only \(for example, approved arrangements for specific medical tracking or documented safeguarding needs\) and must be explicitly authorised by the headteacher.](#)

Any use of mobile devices in school by pupils must be in line with the school's mobile phone policy and acceptable use agreement ([see appendices 1 and 2](#)).

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.

Any mobile devices brought into school must be placed into the class box at the start of the school day, to be collected at the end of the school day. The school takes no responsibility for any devices brought into school.

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)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing 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 IT network manager.

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 behaviour, antibullying, online safety and acceptable use policies. 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 Code of Conduct – Staff Behaviour Policy. 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.

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, e-bulletins 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, **including images generated or altered by AI**, especially around chat groups
 - Sharing of abusive images and pornography, **including images generated or altered by AI**, 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 up the risks
- 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 DDSs 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in [appendix 6](#).

This policy will be reviewed every 2 years by the Executive Board / Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) 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.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct – Behaviour Policy
- Data protection policy and privacy notices
- Complaints procedure
- Computing Policy
- Staff ICT Code of Conduct / Acceptable Use
- Anti-Bullying Policy
- Mobile Phone Policy
- Guidance of use of photography & video equipment by parents/carers
- **AI policy**

Appendix I: EYFS and KSI acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND ONLINE SAFETY: 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 **and** **AI** that a teacher or adult has told me or allowed me to use **and in a way in which a teacher or adult has told me I can use it.**
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - 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
- 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 in a way a teacher or adult has told me**
- Check with my teacher before I print anything
- I will not bring mobile phones or tablets into school



ZIP IT
Keep your personal stuff private and think about what you say and do online.



BLOCK IT
Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT
Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

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

Pupil's Agreement:

I have listened to and understand the ICT and Online Safety Agreement and will follow the rules to keep me and the school safe.

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.

Children will receive lessons and advice on how to keep safe online at school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. The school will help children to learn about staying safe online but recognises that the primary responsibility for online safety at home lies with parents/carers. The school will seek to work with families to help them encourage children to adopt safe use of the digital technologies at home.

I will follow the school's guidance on taking and sharing images and video at school events.

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 usernames 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 • Only use generative AI in a way in which my teacher has taught me inline with the school's AI Policy. • Always log off or shut down a computer when I've finished working on it • The messages I send and write will be polite and responsible.	
I will not:	
• Access websites unless my teacher has expressly allowed this as part of a learning activity, including social networking sites, chat rooms and gaming sites • Access other people's files. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online or using entering information. • Search for, create links to or post inappropriate material including anything created by AI. • Log in to the school's network using someone else's details • Install software on school computers. • Use the school system for gaming, gambling, shopping or uploading videos or music.	
Personal Devices:	
The school cannot accept responsibility for loss or damage to personal devices • It is not permitted for pupils to use Mobile phones during the school day. Phones should be handed to class teacher at the start of the school day and locked away. No Smart Phones are allowed in school. • E-readers, Kindles and cameras should only be brought into school with permission from a teacher and used only with permission. • I agree that if I break the school rules on mobile devices, my device will be confiscated	
I agree that the school will monitor the websites I visit. I understand that the school may take action against me if I am involved in incidents of inappropriate behaviour wherever their location. If the activities are illegal this may be reported to the police.	
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)

WOODLEA PRIMARY SCHOOL – STAFF ICT CODE OF CONDUCT

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher or e-safety coordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes only, or for uses deemed 'reasonable' by the Head or Governing Body / Trust.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that any removable devices I use (e.g. USB memory stick) are password encrypted.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the approved, secure email system for any school business.
- I will ensure that all electronic communications with parents, pupils and staff, including email, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that personal data (such as data held on Arbor) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Governing Body.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location. Unencrypted USB sticks should never be used to store sensitive files for example school reports and IEPs.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network/learning platform without the permission of the Head teacher. No images may be taken using personal or internet enabled devices. I will check the level of permission given by parents/carers of individuals before using or publishing images of children.
- I will not install any hardware or software without the permission of the ICT Team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not contact pupils via any personal devices. Only school email or other professional means of communications should be used. No contact details for pupils should be stored on personal devices.

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school times. They should be switched off or on silent during these times.
- I understand that the school has a right to confiscate any device it has reason to believe is being used inappropriately.
- When taking children out of school, I will use only the school phone in the presence of children and to contact parents or the school if necessary. School phone numbers should be given to parent helpers if they need to contact staff. Personal phones may only be used in an emergency to contact the school/head teacher directly.
- I will **adhere to** the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the ICT Network Manager, the Designated Safeguarding Lead or Head teacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name (Printed):	Job Title:
Signature:	Date:

Appendix 4: Acceptable use agreement (governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR 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
- 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
- Input, upload, or process any personal data of pupils, confidential safeguarding information, or sensitive school data into public or unvetted generative AI tools (such as public AI chatbots or image generators). I will make sure I am aware of approved AI tools for use in school and follow this at all times
- 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
- 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 will 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.

I will use generative AI in line with the school's [AI policy](#).

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

Date:

Appendix 5: Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 6: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident