

WHITGREAVE PRIMARY SCHOOL

ONLINE SAFETY AND ACCEPTABLE USE POLICY



**Mrs Butters - Personal Development and
Online Safety Lead**

Contents

1. Aims	2
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	3
4. Educating pupils about online safety.....	7
5. Educating parents/carers about online safety.....	8
6. Cyber-bullying	8
7. Acceptable use of the internet in school	11
8. Pupils using mobile devices in school	11
9. Staff using work devices outside school	11
10. How the school will respond to issues of misuse	12
11. Training	12
12. Monitoring arrangements	13
13. Links with other policies.....	13
Appendix 1: EYFS and KS1 acceptable use agreement.....	14
Appendix 2: KS2 Acceptable Use Agreement	15
Appendix 3: Acceptable Use Agreement (staff, governors, volunteers and visitors).....	16
Appendix 4: Online safety incident report log	18
Appendix 5: Requesting filtering to be removed.....	19

1. 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.
- 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 in and escalate incidents.

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, antisemitism, 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 scams.

Online safety is a safeguarding issue and forms a core part of the school's whole-school safeguarding approach. The school recognises that many safeguarding risks can occur online as well as offline.

2. 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](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Generative AI: product safety expectations - GOV.UK](#)

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 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 and staff meetings), at least annually or as required with any new updates. This will ensure that all staff are continually provided with the relevant skills and knowledge to effectively safeguard the children.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, 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 that appropriate filtering and monitoring systems are in place on all school devices and networks. Their effectiveness will be reviewed regularly. 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 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 their safeguarding needs.
- > The governor who oversees online safety is Jayne Pownall.

All governors will:

- > Ensure 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 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.
- > Receive regular assurance reports regarding filtering, monitoring, cyber security and online safety trends.

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 (DSL)

Details of the school's Designated Safeguarding Lead (DSL) and deputies (DDSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL alongside the DDSL and Online Safety Lead takes 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.
- 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, ICT 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's child protection policy.
- Ensuring that any online safety incidents are logged on CPOMS if they relate to safeguarding concerns, or on the Online Safety Incident Report Log if they relate to technical issues (see appendix 5). These are then 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, Online Safety Group 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.
- Testing and monitoring the filtering and monitoring systems and ensuring any concerns are dealt with.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

An annual review of filtering and monitoring systems will be undertaken by the senior leader responsible for filtering and monitoring, supported by the DSL, Online Safety Lead and ICT support. A written record of this review will be maintained.

Filtering and monitoring reports will be reviewed regularly by the DSL and DDSL responsible for filtering and monitoring and any safeguarding concerns identified through these systems will be acted upon promptly.

3.4 The ICT manager

The ICT 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 half termly 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 (see appendix 4) and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

The school recognises that cyber security forms part of safeguarding. Appropriate measures will be implemented to protect school systems, personal information and access to educational resources.

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.
- 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, DDSL and Online Safety Lead are 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 completing the filtering and monitoring report (appendix 4) and sending this to the DSL, DDSL or Online Safety Lead.
- Following the correct procedures by completing the 'Requesting filtering to be removed' form (appendix 5), 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 on CPOMS. If an inappropriate website is accessed on school equipment the 'Online safety incident report' form (appendix 4) should be completed and sent to the Online Safety Lead, Gemma Butters or Nichola Parker and these will be 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.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.

Parents/carers 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](#)
- Parent resource sheet - [Childnet](#)
- National Online Safety
- Internet Matters
- CEOP

3.7 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:

- A planned online safety curriculum will be delivered through Computing, Personal Development and other relevant lessons. These will be regularly revisited. (The school currently uses Project Evolve and EC Publishing).
- Key online safety messages should be reinforced through planned assemblies and morning activities.

In **Key Stage (KS) 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 (KS) 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.
- 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.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The impact of their online activity on their digital footprint and online reputation.
- How to identify misinformation, disinformation, manipulated media and unreliable online content.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Pupils should be encouraged to report any online safety concern regardless of whether it occurs on school equipment, personal equipment or outside school hours.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters and other communications sent home, and in information via our website.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL/DDSL or Online Safety Lead.

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. (See also the School Behaviour Policy).

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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal Development (PD) 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.

The school also sends information/leaflets on cyber-bullying to parents/carers so 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.

Online abuse may include child-on-child abuse, harassment, harmful sexual behaviour, sharing of nude and semi-nude images, coercion, exploitation, bullying and digitally manipulated imagery. This includes AI-generated or digitally manipulated nude and semi-nude images, sometimes referred to as 'deepfake' or 'deep nude' images.

6.3 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 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 a criminal offence

If a member of staff believes that a child's phone has harmful content, is being used to commit an offence or cause harm to another person, the Headteacher (or a person designated by her) will be called and they will decide if it is necessary to confiscate the device. Parents will then be contacted to assist in investigating the incident. If during the investigation with parents, inappropriate content is found, safeguarding procedures will be followed.

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 Headteacher or appropriate staff member
- Explain to the pupil/staff why they are being searched, contact the parents if the situation is involving a pupil and explain how the search will happen (involving the parents in this), and give them the opportunity to ask questions about it
- Seek the staff/ pupil's co-operation

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 criminal 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/carer 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 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](#).

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](#).

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)

At Whitgreave Primary we understand the valuable potential that Artificial Intelligence (AI), including generative AI, holds for schools. We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

- This policy covers the use of AI tools by school staff, governors and pupils. This includes generative chatbots such as ChatGPT and Google Gemini (please note, this list is not exhaustive). It also includes open and closed AI tools.
- **Open generative AI tools** are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information.
- **Closed generative AI tools** are generally more secure, as external parties cannot access the data you input.

Pupils' work must not be used by staff to train generative AI models without appropriate consent or exemption to copyright.

Staff must not input personal data, safeguarding information, pupil records, SEND information, staff records or other confidential information into public generative AI tools unless the tool has been approved by the school and appropriate data protection assessments have been completed.

Any AI-generated output used by staff must be reviewed by a member of staff and not relied upon without human oversight. AI-generated content may contain inaccurate, biased or misleading information and should not be accepted without verification.

Whitgreave Primary School recognises that AI 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, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include

someone's likeness. Whitgreave Primary School will treat any use of AI to bully pupils in line with our behaviour policy.

AI sites are monitored and filtered within the schools filtering and monitoring systems. They are regularly checked to ensure they are still appropriate for pupils.

Pupils will be taught about the potential risks and benefits of using AI in Online Safety and Personal Development lessons.

They will be taught about:

- deepfakes
- misinformation and disinformation
- AI chatbots
- AI-generated images
- manipulation of digital content
- responsible use of AI tools

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 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.

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 3.

8. Pupils using mobile devices in school

The school is a mobile phone-free environment. Pupils must not have access to mobile phones or smart devices during the school day, including lessons, transitions, breaktimes, lunchtime, trips, visits or any other activities organised by the school. Any exceptions must be agreed by the Headteacher.

All mobile phones must be **handed in to the class teacher or school office at the beginning of the school day**. Phones will be kept safely and **returned to the child at the end of the school day**.

We appreciate parents and pupils supporting the school in maintaining a safe, focused and mobile phone-free environment.

9. 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/memory stick 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.
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

If staff have any concerns over the security of their device, they must seek advice from Nichola Parker or Gemma Butters who will ensure Spark IT investigate the issue further.

10. 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. 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. 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, threatening, 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 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 deputies will undertake child protection and safeguarding training, which will include online safety, at least every two 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.

12. Monitoring arrangements

The DSL and Staff will log behaviour and safeguarding issues related to online safety. These will be logged on CPOMS and Online Safety will be tagged.

This policy will be reviewed yearly. 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.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct and disciplinary procedures
- Data protection policy
- Complaints procedure

Appendix 1: EYFS and KS1 acceptable use agreement

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 (such as computers and iPads) 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:
 - I select 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 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 or the area my teacher asks me to
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it, when my teacher tells me.

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:

Appendix 2: KS2 Acceptable Use Agreement

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 iPads) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly
- 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 that might upset, distress or harm me or others
- Always log off or shut down a computer when I've 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
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Use AI systems without permission from a teacher.
- Input personal, school or work information into AI systems.
- 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
- Input any personal information or images of myself or others into AI systems

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

- I will not use it during lessons, clubs or other activities organised by the school.
- I will hand in my device each morning to be stored securely.
- I will not take photos or recordings (either video or audio) of school staff or other pupils without their consent.

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:

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 that 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
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking permissions first or with the class teacher
- 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
- Input personal data, or any other confidential school information into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT, Copilot and Google Bard)
- Use personal accounts to access AI tools for school business unless authorised by the school.

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

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will:

- Agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- Only take photos on a school device, unless previously agreed by the Headteacher
- Lock devices when not working on them
- 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
- Let the Designated Safeguarding Lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material
- Use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too
- Ensure that any personal data stored on memory sticks is encrypted and kept secure
- Not share children's personal information on AI systems
- Pupils' work must not be used by staff to train generative AI models without appropriate consent or exemption to copyright.
- Not share my device among family or friends
- Keep operating systems up to date by always installing the latest updates
- Be alert to phishing emails and alert the Network manager if I believe I have received one
- Ensure that use of a personal mobile phone is restricted to non-contact times
- Verify any AI-generated content before using it for educational or professional purposes.

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

Date:

Appendix 4: Online safety incident report log

Date:	
Lesson/Classroom:	
Device used:	
What was found?- Website/Image found:	
Please explain circumstances of image/website being found e.g. google search, website search etc. Please be as specific as possible.	
Person reporting incident:	
Action taken by DSL/Online Safety Lead/Computing Lead:	

Appendix 5: Requesting filtering to be removed

Date:	
Lesson/Classroom/teacher:	
Device to be used:	
What website or key words need to be unblocked?	
Please explain why this is needed e.g curriculum area/lesson etc	
Temporary or permanent? If temporary please give a date when it can be blocked again	
Person reporting incident:	
Action taken by DSL/Online safety Lead/Computing Lead:	

