

Sharpness Primary School

Online Safety Policy



Approved by:	Miss H Buckingham, Headteacher Mrs Sara Matthews, Chair of Governors	Date: 10 th April 2026
Last reviewed:	April 2026	
Next review due by:	April 2027	

Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school.....	7
8. Pupils using mobile devices in school	7
9. Staff using work devices outside school.....	8
10. How the school will respond to issues of misuse	8
11. Training.....	8
12. Monitoring arrangements.....	9
13. Links with other policies.....	9
Appendix 1: acceptable use agreement (pupils and parents/carers)	10
Appendix 2: acceptable use agreement (staff, governors and volunteers)	12
Appendix 3: online safety training needs – self audit for staff	14
Appendix 4: online safety incident report	

1. Aims

- Have robust processes in place to ensure online safety
- Identify and support vulnerable pupils at greater risk online
- Include mobile and smart technology risks
- Establish clear mechanisms to respond to incidents

Our school aims to:

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 seminudes and/or pornography), sharing other explicit images and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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](#)

➤ [Meeting digital and technology standards](#)

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, 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, 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 the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with appropriate staff 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: Anya Sahla

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 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

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 DSL and deputies 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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the IT manager (Focus Networks) and other staff, as necessary, to address any online safety issues or incidents
- Working with the 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
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Managing all online safety issues and incidents in line with the school child protection 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 4 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 governing board
- 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
- Carry out annual online safety risk assessments

This list is not intended to be exhaustive.

3.4 The IT manager – Focus Networks

The IT manager is responsible for:

- Putting in place an appropriate level of security, 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 IT 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 IT 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 (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

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

- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Know how to report concerns
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Behaviour policy
- Responding appropriately, in line with the school's Child Protection and Safeguarding policy, to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Understand filtering/monitoring systems

This list is not intended to be exhaustive.

3.6 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 IT systems and internet (appendix 1)

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](#)
- Online safety topics for parents/carers – [Childnet](#)
- Parent resource sheet – [Childnet](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT 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 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

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 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.
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- The emerging risks of AI including deepfakes awareness and risks associated with AI-generated content.
- The importance of cyber security including: password security, phishing and scams and the need for multi-factor authentication.

All schools - the safe use of social media and the internet will also be covered in other subjects where relevant including social media age restrictions and the risks of sharing content online.

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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. There will also be opportunities for parents/carers to attend online safety talks, hosted by the school. This policy will also be shared with parents.

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

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 (see also the school's 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. Class teachers will discuss cyber-bullying with their class groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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).

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

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 headteacher / DSL / appropriate senior staff member
- 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 DSL / 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), 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)

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.

Sharpness recognises 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', 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.

Sharpness will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policy (at next review).

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

7. Acceptable use of the internet in school

All pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). 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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

If agreed with the Headteacher, pupils may bring mobile devices into school; this includes smart watches or any other smart device but these must be stored securely in the office. This includes devices with a school mode function.

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

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.

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 – the strongest passwords are 3 random words.
- 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
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- 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 2.

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 the Headteacher

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT 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 IT 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 which 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 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the Headteacher. 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

Anti-bullying

Behaviour

Child Protection and Safeguarding

Complaints Procedure

Data Protection Policy and Privacy Notices

Relationships and Sex Education (RSE)

Remote Learning Plan

SEN

Staff Disciplinary Procedures

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

Technologies and the Internet, including social media, are powerful tools which provide excellent opportunities for learning and teaching. They can motivate learners, promote creativity, and support effective learning, assessment and engagement with parents. All users have an entitlement to good, safe access to technology and the Internet.

This Acceptable Use Policy is intended to ensure:

- You are aware of what the school is doing to help your child become a responsible user of technology and stay safe at school
- You are aware of the importance of living safely online and are able to support your child with keeping safe and behaving well online.

The school will aim to ensure your child has good, safe access to IT for learning and, in return, expects your child to use the equipment responsibly.

Content

- Your child should know that all school IT systems are intended for educational use and not their own personal use.
- They should only access materials which are appropriate to their education.
- They should not undertake any activity which threatens the integrity of the school IT systems, or which attacks or corrupts any other systems.

Contact

- Your child should communicate online in an appropriate manner and tone and not use aggressive or inappropriate language.
- They should only communicate information relating to school activities using official school systems.
- They should not use their personal email addresses on the school IT systems.
- They should only use their own user names and passwords, which will not be shared with anyone else.

Conduct

- Your child should not try to bypass the Internet access filtering in place in school or access sites that are illegal.
- They should only use their personal IT in school for legal activities and follow the rules set out in this agreement when using it.
- They should only take images or video of pupils or staff where it relates to school led educational activities and will ensure they have permission before they take them.
- They should not install programmes on a school device.
- They should not try to alter computer settings.
- They should not cause damage to IT equipment in school and will immediately report any damage or faults involving equipment or software.
- They should tell you or a member of staff if an issue arises in or out of school that might compromise learner, user or school safety.

Taking Digital Film and Images

- Children and staff may use school digital devices e.g. iPads, Chromebooks to record school activities.
- The school complies with the Data Protection Act (2018).

Problems or Concerns

- Any issues you are made aware of with use of technology in school should be reported immediately to a child's teacher so that appropriate steps can be taken.
- If your child does not behave appropriately online, then the school will take steps to deal with this as with any other issue with behaviour.
- You are obviously responsible for your child's safety online when at home and we would hope you will be discussing this with your child.

Acceptable Use Agreement

We request that you sign the permission form below to show your support of the school in helping to keep your child safe. By signing this form you are agreeing that:

- Your child will use school technology and online services for learning as outlined above
- You have read and discussed the rules with your child
- You understand the rules that your child should be following when using IT in school

Pupil name (print):

Parent / Carer name (print):

Signed:

Date:

Additionally, the Information Commissioner's Office has stated that, parents / carers may take videos and digital images of their children at school events for their own personal use. However, such images and videos must not be published or made available on social networking sites in order to protect other children and respect privacy.

- Parents are asked not to post photos or videos of other children (not their own) without the permission of their parents
- Parents / carers should also not comment negatively on any activities involving other pupils in digital / video images, including on social media platforms.

Please sign below to indicate that you have read and understood the above agreement about images and videos and agree to abide by it.

Parent / Carer name (print):

Signed:

Date:

Appendix 2: acceptable use agreement (staff, governors and volunteers)

Technologies and the Internet, including social media, are powerful tools which provide excellent opportunities for learning and teaching. They can motivate learners, promote creativity, and support effective learning, assessment and engagement with parents. They also bring opportunities to enhance teaching, increase staff efficiency and provide opportunities for staff to benefit from professional development through networking and collaboration. All users have an entitlement to good, safe access to technology and the Internet.

Content

- I know that all school IT systems are intended for educational use and not my own personal use.
- I will only access materials which are appropriate to staff professional development or pupils' education.
- I will not undertake any activity which threatens the integrity of the school IT systems, or which attacks or corrupts any other systems.

Contact

- I will communicate online in an appropriate manner and tone and I will not use aggressive or inappropriate language.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will only use my own user names and passwords, which will not be shared with anyone else.
- I will not 'friend' pupils on social networking sites or accept 'friend' requests.

Conduct

- I will not try to bypass the Internet access filtering in place in school or access sites that are illegal.
- I will only use my personal IT in school for legal activities and I will follow the rules set out in this agreement when using it.
- I will not use the school's IT in any way which could harm the school's reputation.
- I will not use my personal equipment to store images or video of pupils.
- I will only take images or video of pupils or staff where it relates to agreed learning activities and will ensure I have permission before I take them. If these are to be published online or in the media, I will ensure that parent or staff permission allows this.
- I will not install programmes on a school device unless I have permission.
- I will not try to alter IT equipment settings, unless this is allowed in school policies.
- I will not cause damage to IT equipment in school and will immediately report any damage or faults involving equipment or software.
- I will take all reasonable steps to ensure that work devices are secure and password-protected.
- I understand that I am also bound by the requirements of the school's data protection policy and procedures.
- I will take immediate action in line with school policy if an issue arises in or out of school that might compromise learner, user or school safety.

Commerce

- I will not promote private businesses through any school channel/platform, or in my professional capacity, unless that business is directly related to the school.

Safeguarding

- I will immediately report any illegal, inappropriate or harmful material, or incident I become aware of, to the head teacher.
- If I believe a member of staff is infringing this policy, or putting themselves or others at risk, I will report this to the head teacher.
- If I believe a young person may be at risk, I will follow the safeguarding procedures.

- If I believe a young person may be being bullied via technologies, I will follow the anti-bullying procedures.

This policy should be read in conjunction with other school policies, particularly the Data Protection policy and procedures. As well as the Safeguarding and Child Protection policy.

This agreement links to:

Gloucestershire Safer Working Practice Guidance

Part Two of Keeping Children Safe in Education 2021 on Online Safety (paragraphs 123 – 135) and Annex D

Sexual violence and sexual harassment between children in schools and colleges (DfE) September 2021

Sharpness Primary School Remote Learning Plan

Acceptable Use Agreement

I accept and agree to abide by the terms of the Acceptable Use Agreement as laid out above.

Full name (print):

Signed:

Date:

Appendix 3: 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/carers?	
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 4: 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