Online Safety Policy

Horwich Parish CE Primary School

Approved by: Pupils Community and Parish Committee	**Date: Autumn 2025**
Author: Mrs R Woods and Mrs D Mills	**Version: 1**
Last reviewed on:	**Autumn 2024**
Next review due by:	**Autumn 2026**

Version Control

Current version	Previous version	Summary of changes made
May-22	Jun-21	Frequency of review changed to every 2 years
Sep-22	May-22	Updates reflect changes to KCSIE 2022. Updates reflect changes to DfE guidance on searching, screening and confiscation 2022.
Sep-22	Sep-23	Updates reflect changes to KCSIE 2023. Reference made to filtering & monitoring (section 3.5).
Sep-22	Sep-23	Removal of appendix 4 – in line with SENSO reports received by DSL weekly.
Sep-22	Sep-23	Frequency of review changed to annually.

Our vision is to be a school where everyone can achieve and "let their light shine" both individually and collectively as a community.

Learning to love each other as Jesus loved us, respecting each other and growing into the people God has called us to be.

Contents

Appendix

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'); and
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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

It also refers to the DfE's guidance on protecting children from radicalisation and Meeting Digital and Technology Standards in Schools and Colleges.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has

given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The governor who oversees online safety is Sue Baines, Chair of Governors.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with 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

Details of the school's designated safeguarding lead (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:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the head teacher, ICT manager/provider (Benchmark) 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.
- Ensuring that any online safety incidents are logged (SENSO reports received weekly by the DSL) 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 3 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 head teacher and/or governing board.

This list is not intended to be exhaustive.

3.4 The IT Manager

The IT manager is Benchmark North they are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting security checks and monitoring the school's IT systems on regular basis.
- Ensuring that any online safety incidents are logged and sent to the Head/DSL to be dealt with appropriately in line with policy.
- Ensuring that any incidents of cyber-bullying are logged and sent to the Head/DSL to be dealt with appropriately in line with the school behaviour policy.
- Computeam Limited provide our internet and web filtering system and are responsible for blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

3.5 Filtering & Monitoring

In line with the KCSIE 2023 update, our school have reviewed and actioned the guidelines referenced for feedback and monitoring.

- Benchmark North to ensure the filters we have in place are effective and not limiting to teaching and learning.
- Staff to be transparent with pupils regarding the filtering system used; they must understand that their internet use in school is tracked.
- Governing body to be responsible for reviewing the effectiveness of the systems in place.
- DSL and relevant staff to have a good understanding of the filtering and monitoring system.

More information can be found here: Additional guidance on "appropriate" filtering and monitoring can be found at: UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/teachers-and-schoolstaff/appropriate-filtering-and-monitoring.

3.6 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 and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2);
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy; and
- 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.

3.7 Parents

Parents are expected to:

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

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

3.8 Visitors and Members of the Community

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

4. Educating Pupils About Online Safety

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

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.

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 safe use of social media and the internet will also be covered in other subjects where relevant.

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

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. 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 the head teacher.

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 1 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. Class teachers discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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.

The computing curriculum for every year group begins with digital citizenship, maintaining online safety as a clear priority.

6.3 Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in your behaviour policy – adapt to e.g., specify which staff are authorised), 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 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; and
- Seek the pupil's cooperation.

At the request of the head teacher, 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 headteacher 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 Head teacher immediately, who will decide what to do next. The Head teacher 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
- Our behaviour policy/searches and confiscation 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.

7. Acceptable Use of the Internet in School

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

More information is set out in the acceptable use agreements in appendices 1 to 2, also see the separate acceptable use policy.

8. Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them during the school day: mobile phones are to be switch off before entering the school building and place in a container which is kept in the office during the school day.

Any use of mobile devices in school by pupils must be in line with the 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.

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 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.

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 relevant role of individual, e.g., head teacher or the business manager.

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 and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures & 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, harassing, and misogynistic messages;
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups; and
    - 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; and
- 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.

This policy will be reviewed annually by Debbie Mills. 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.

13. Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy

Appendix A: EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)

EYFS, Year 1 and Year 2 Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ iPads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
 My Online Safety	• I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
 Using the Internet @school	• I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
 Using the Internet @home	• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • Where I have my own username and password, I will keep it safe and secret. • I will tell a trusted adult if I see something that upsets me on the screen. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that these rules help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

_____**Child's Signature**

Parents/Carers:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

_____ _____

Parent/Carer's Signature **Date**

Appendix B: KS2 Acceptable Use Agreement (Pupils and Parents/Carers)

Year 3 and Year 4 Pupils School Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ iPads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 Using the Internet @school	• I will only visit sites that are appropriate to my learning at the time **My School Accounts** • I will keep my username and password safe and secure - I will not share it. • I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may use it. **My role as a Digital Citizen.** • I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
 Using the Internet @home	• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) • I will immediately report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g., CEOP, Childnet, Childline, Barnardo's. **My Communications** • I will be aware of the "SMART" rules, when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use inappropriate language and I understand that others may have different opinions. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

_____

Child's Signature

Parents / Carers:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

_____ _____

Parent/Carer's Signature **Date**

Appendix C: KS2 Acceptable Use Agreement (Pupils and Parents/Carers)

Year 5 and Year 6 Pupils Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ iPads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 Using the Internet @school	• I will only visit sites that are appropriate to my learning at the time **My School Accounts** • I will keep my username and password safe and secure - I will not share it. • I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may steal it. **My role as a Digital Citizen.** • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images of anyone without their permission.
 Using the Internet @home	• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) • If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardo's. **My Communications (Including texting and messaging)** • I will be aware of "stranger danger", when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

_____ Child's Signature

Parents / Carers:

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

_____ _____

Parent/Carer's Signature **Date**

Appendix D: 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?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
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?	