Rosh Pinah Primary School

Online Safety Policy

Updated: September 2024
Date for Review: September 2025

CONTENTS

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 than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole School Community in its use of technology including mobile and smart technology (which we refer to as 'mobile phones')
- Have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues
- Ensure we have a robust filtering and monitoring arrangements in place to safeguard pupils and staff from potentially harmful and inappropriate online material
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. The four key categories of risk

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

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying, and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) Statutory Safeguarding Guidance, 'Keeping Children Safe in Education 2024' and its advice for Schools on:

- Teaching online safety in Schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and School staff
- Relationships and sex education
- Searching, screening and confiscation.

It also refers to the DfE's guidance on protecting children from Radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

4. Roles and responsibilities

4.1. The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

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 the 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 SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Ensure children are taught how to keep themselves and others safe, including keeping safe online
- Ensure 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
- Ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Governing Body will review the DfE filtering and monitoring standards, and discuss with the Senior Leadership Team and IT technician and service providers what needs to be done to support the school in meeting those standards, which include the following:
  - 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 the online safety is Mrs Nicole Blech.

4.2. The Headteacher will:

- Ensure that staff understand this Policy and that it is being implemented consistently throughout the school
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented
- Understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with the IT technician and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE 2024.

4.3. The Designated Safeguarding Lead

Details of the School's DSL and Deputy DSL are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the Headteacher, ICT technician 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 in CPOMS 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 School Behaviour Management Policy
- Taking the lead in understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT technician to make sure the appropriate systems and processes are in place
- Communicating regularly with the SLT and the Safeguarding Governor/Committee to discuss current issues (anonymised), review incident logs and discuss how filtering and monitoring work have been functioning
- 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 Headteacher and/or Governing Body
- Undertaking annual risk assessments that consider and reflect the risk children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

4.4. The ICT Technician

The ICT technician is responsible for:

- Putting in place 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
- Blocking access to potentially dangerous sites and where possible, preventing the downloading of potentially dangerous files
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Ensuring that any online safety incidents are immediately reported to the DSL or Deputy DSL
- Ensuring that any incidents of cyber-bullying are immediately reported to the DSL or Deputy DSL and dealt with appropriately in line with the Behaviour Management Policy.

4.3. 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)
- Working with the DSL to ensure that any online safety and cyber-bullying incidents are logged using CPOMS 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 Management Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online, offline and maintaining an attitude of 'it could happen here'
- Following the correct procedures by speaking with the DSL and ICT technician if they need to bypass the filtering and monitoring systems for educational purposes
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of online safety.

4.4. Parents/ carers

Parents/ carers are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the School's ICT systems and internet (Appendices 1 and 2)
- 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 factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

4.5. 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).

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the Curriculum.
All primary schools will have to teach:

- Relationship, sex and health education

Pupils in Key Stage 1 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

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The boundaries that are appropriate in friendships with peers and others (including in a digital context).

The safe use of social media and the internet will also be covered in other subjects where relevant. The School will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may invite speakers to talk to pupils about this. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Educating parents about online safety

The School will raise parents' awareness of internet safety via email, weekly newsletter, school website and Facebook page. This Policy will also be shared with parents and carers.

The school will let parents/carers 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 class teacher or DSL/ Deputy DSL.

Concerns or queries about this policy can be raised with the Headteacher.

7. Cyber-Bullying

7.1. 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 Management Policy).

7.2. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed effectively.

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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Management 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 School also sends information 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.

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.

7.3 Examining electronic devices

The Headteacher and any members 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/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 or Deputy DSL
- 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 devise 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, staff must reasonably suspect that the device has been, 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 or other member of the Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and /or
- The pupil and / or the parent / 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 / Deputy DSL 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 screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- The school's Behaviour Management 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.

7.4 Artificial intelligence (AI)

Generative aritificial 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 Bard.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others e.g. in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully pupils in line with our Anti-bullying and Behaviour Management Policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

8. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and Governors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet (Appendices 1-3). Visitors will be expected to read and agree to the School's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Use of the School's internet must be for educational purposes only, or for fulfilling the duties of an individual's role. The School 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.

9. Pupils using mobile devices in school

Year 6 pupils may bring mobile devices into School, but in line with the Mobile Phone Policy are not permitted to use them on the School premises during:

- Lesson break or lunch time
- Clubs (before or after school), or any other activities organised by the school.

Pupils must leave their mobile phone (switched off) at the school office at the start of the day and collect it again at the end of the school day. The school will not accept responsibility for a mobile phone, which has been brought into school.

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.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device secure and password-protected. They do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside School
- Any USB devices containing data relating to the School must be 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.

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

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

11. How the School will respond to issues of misuse

Where a pupil misuses the School's ICT systems or internet, we will follow the procedures set out in our Child Protection and Safeguarding Policy and Behaviour Management Policy. 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.

12. Training

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

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

The DSL and Deputy DSL 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. More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

All staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

13. Filtering and monitoring arrangements

Filtering is the system a school uses to restrict what access a student has to the internet, e.g. blocking certain sites. Filtering should reduce the amount of access or exposure students have to harmful material.

The school has educational filtered secured broadband connectivity through LGFL, which has sophisticated, school safe, fully compliant web filtering as per KCSIE 2024. The LGFL filtering systems, blocks sites that fall into categories such as pornography, race hatred, gaming, sites of all illegal nature etc.

Monitoring is very simply keeping watch on what students are doing whilst they are online. We follow different ways to implement monitoring strategies e.g.

a) Physical monitoring where staff directly monitor students use e.g. circulating during a computer lesson. They check websites, apps and search results to understand age ratings and ensure privacy settings are set at the highest level by liaising with the IT technician
b) Software monitoring, often based on certain key searches or terms. The software systems are regularly reviewed interpreted and have alerts that are prioritized for intervention.

A review of filtering and monitoring is carried out to identify the current provision, any gaps, and the specific needs of pupils and staff. The DSL monitors all logs of behaviour and safeguarding issues related to online safety on CPOMs. Staff incidents should be reported immediately to the Headteacher and the incident recorded on the report log found in appendix 5.

This policy will be reviewed annually. At every review, the policy will be shared with the Governing Body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with Other Policies

This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Management and Bullying Policy
- Mobile Phone and Smart Device Policy
- Remote Learning Policy
- Mental Health and Wellbeing Policy
- Staff Disciplinary Procedures
- Data Protection Policy
- Complaints Procedure
- Acceptable Use Agreement

Appendix 1: EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)

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

I will read and follow the rules in the acceptable use agreement policy
When I use the School's ICT systems (like computers) and get onto the internet in School I will:
• 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 click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use School computers for School work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it.
 	
I agree that the School will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (Pupil):	**Date:**
Parent/Carer Agreement: I agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of School staff. I agree to the conditions set out above for pupils using the School's ICT systems and internet, and will make sure my child understands these.	
Signed (Parent/Carer):	**Date:**

Appendix 2: KS2 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of Pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the School's ICT systems (like computers) and get onto the internet in School I will:** • Always use the School's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it. **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision. **If I bring a personal mobile phone or other personal electronic device into School:** • I will not use it during lessons, clubs or other activities organised by the School, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online. **I agree that the School will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (Pupil):	**Date:**
Parent/Carer Agreement: I agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of School staff. I agree to the conditions set out above for pupils using the School's ICT systems and internet, and will make sure my child understands these.	
Signed (Parent/Carer):	**Date:**

Appendix 3: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of Staff Member/Governor/Volunteer/Visitor:	
When using the School's ICT systems and accessing the internet in School, or outside School on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the School's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the School's network • Share my password with others or log in to the School's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the School, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the School.	
I will only use the School's ICT systems and access the internet in School, or outside School on a work device, for educational purposes or for fulfilling the duties of my role • I agree that the School will monitor the websites I visit and my use of the School's ICT facilities and systems • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside School, and keep all data securely stored in accordance with this policy and the School's Data Protection Policy • I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material • I will always use the School's ICT systems and internet responsibly, and ensure that pupils in my care do so too	
Signed (Staff Member/Governor/Volunteer/Visitor):	**Date:**

Appendix 4: 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?	
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 5: 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**