Online Safety Policy

APPROVED BY:	**Tracey Smith**
APPROVED BY SIGNATURE (Headteacher):	
DATE APPROVED:	**October 2024**
REVIEW CYCLE:	**Bi-annually**
DATE OF NEXT REVIEW:	**October 26**

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')
- 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.

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 and the Online Safety Act 2023.

3. Roles and responsibilities

3.1 The governing body

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

The governing body 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 body 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 body 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 body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body 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 body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

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 2)
- 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 ALL 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 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 Headteacher and governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT technician and the IT provider to make sure the appropriate systems and processes are in place
- Working with the Headteacher, IT technician, IT provider, IT coordinator 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 through Smoothwall and / or My Concern 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 Headteacher and/or governing body
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The IT Technician and Chestnut Infrastructure

The IT Technician and Chestnut Infrastructure are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a daily basis and Watchguard monitors constantly

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring 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

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 ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by completing a My Concern including the date, time and details of what has happened.
- Following the correct procedures by asking permission from the Headteacher and speaking to IT support, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- 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
- Hot topics – Childnet
- Parent resource sheet – Childnet
- School sends home monthly online safety newsletters from the Knowsley group, which give up to date developments on topics linked to online safety

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:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

We are an all age special school and we teach online safety as part of the omputing curriculum, our pupils access work at least a Key Stage below their chronological age. Some of our pupils will not be able to understand some of the more complex aspects of online safety, where as others will.

In **Primary**, 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 3** 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
- 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

In **Key Stage 4**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 5** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of Key Stage 4 and Key Stage 5**, most pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

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

Our pupils complete a Monday Big Question every Monday, within their class setting. This enables them to explore topics of interest as a class and discuss what they think. This enables staff to challenge inaccurate perceptions and reinforce safety. The Monday Big Question has been used to gather the pupils thoughts on online safety, the feedback is in Appendix 4.

5. Educating parents/carers about online safety

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

Online safety will also be covered during parents' evenings.

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

If parent's/carer's 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 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 classes and specific workshops are run by the Phase Leads and by the Police.

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 bulletins on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected. Phone calls are made to parents/carers to highlight the issues that arise within school and ensure that they know to check social media and messaging apps for contacts the pupils do not know.

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.

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 or 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 co-operation

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 Headteacher and DSL 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 Headteacher 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
- Our Behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

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

Rigby Hall School 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.

Rigby Hall School will treat any use of AI to bully pupils in line with bullying in our Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

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

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

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

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

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Playtimes
- Clubs before or after school

Some pupils in Post 16 may be allowed to use their mobile phones when out in the community but this will be part of the risk assessment and a discussion around safe usage had before leaving the site.

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 that 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 Chestnut Infrastructure and the ICT technician.

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. This may include the removal of internet access in school.

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

11. Training

All new staff members will receive training via SSSCPD, 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

Behaviour and safeguarding incidents linked to online safety are logged on My Concern and are triaged by the DSL and DDSL's.

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment, 360 Degree safe 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 1: acceptable use agreement (pupils and parents/carers)

Acceptable Use Policy – PUPILS

- I will ask an adult if I want to use a computer
- I understand that the systems I use will be monitored and checked.
- I will keep my personal information safe such as my password and will not share it with anyone
- I will not interfere with the way that others use technology. This includes using someone's else password (even with permission) or altering their files/work. I understand that this is a violation of the Computer Misuse Act 1990.
- If I leave my laptop unattended then I must lock it. This is so no one can access my account
- I will not use my own personal devices such as memory sticks and mobile phones. I understand my phone must be handed in and it must not be used at all during the day.
- I will only use the laptop for education purposes only. Whilst on it, I will not try to deliberately bypass any systems designed to keep myself and the school safe.
- I will look after the IT equipment and will report any damages to my class teacher immediately however this may have happened.
- I will tell a trusted adult if I think I have done something wrong or am upset by what I have seen online.
- I will not attempt to download anything without permission. If I need any software then I must talk to my teacher. I know that only the IT team can download software that I may need.
- I understand that if I break any of these rules then I won't be able to use the computer and my account will be disabled.

I have read and agree to the terms and conditions in this agreement. Please sign overleaf.

Child's name: _____

Child's signature: _____

Parent/guardian name: _____

Parent/guardian signature: _____

Date: _____

Appendix 2: Acceptable User Policy Staff / Governors

Acceptable Use Policy – STAFF / Governors

- I will utilize the school's IT equipment solely for official school purposes that align with my job role.
- I acknowledge that the school will monitor my use of the IT systems, including email and print usage and reserves the right to investigate my usage.
- I have carefully read and understood the E-safety and Online Safety and Data Protection policies.
- I will use a strong password of at least 10 characters to include upper case, lower case, numbers and special characters.
- I will not divulge my password to any individual, nor will I use anyone else's password, even with their permission.
- I will lock my computer every time if I leave it unattended.
- I will not access, modify, copy, or delete any other user's files unless I have explicit permission from the owner. Failure to comply with this will be a violation of the Computer Misuse Act 1990.
- I will notify the appropriate personnel immediately through proper channels of any damage or faults involving IT equipment, however it happens.
- I will not engage in any illegal, inappropriate or harmful material. This includes uploading, downloading, storing, or distributing either in school or off-site.
- I will not disable or bypass any filtration or restriction system established to guarantee my safety and that of the school.
- I will not plug in my personal devices to the school network.
- I will not use memory sticks, encrypted or otherwise.
- I will ensure that I obtain consent and strictly follow the school's procedures for taking and publishing images of others.
- I will exclusively use the school's designated communication systems to communicate with parents and pupils. I shall refrain from using any inappropriate or aggressive language and will ensure that all interactions are conducted in a respectful and courteous manner.
- I will not open any attachments to emails unless the source is known and the sender is trusted.

- I will ensure that I regularly stay up to date with cybersecurity and familiarise myself with the threats that a school can face. I know what to do if I think I have encountered a threat.
- I understand that my laptop and iPad may be recalled for updates and maintenance.
- I will make it a priority to ensure the safety and security of important information.
- I will not dispose of any IT equipment – I will hand it in to the IT Technician or Business Manager.
- I will not attempt to download anything without permission. I understand that only the IT team can download software that I may need.
- I will ensure that no other person can see school information when I am using my laptop offsite, for example at home.
- I acknowledge and understand that I am solely responsible for my actions while utilizing the IT equipment of the school, regardless of whether I am present on or off the school premises.

I understand that if I fail to comply with any point on this Acceptable Use Policy then I may face disciplinary action. My account may be disabled and local bodies such as the Governors and Police may be involved.

I have read and understand this Acceptable Use Policy and agree to use the IT system following these guidelines.

Staff Name:	
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 : Our pupil voice about online safety.

These views were gathered by class staff through our Monday Big Question, the pupils were asked:

“What is online safety?”
“What can school do to help children be safe online?”
“What would you like to see in school to keep you safe online?”

Our pupils know that they should not share their information with people online and that they should not add people they do not know online.

“Don’t talk to strangers, block people that you do not know”
“Don’t give out personal information”

Our pupils think school should block sites that are not safe and make sure they cannot access them. They know that we check what they are watching or searching through our filtering and monitoring systems.

“Watch at school what people have been searching”
“Block certain things so people can’t see what’s not safe”

Our pupils know that we teach online safety to keep them safe.

“They only keep teaching us to keep us safe.”

Our pupils know that they should report to staff if they have online safety worries and not just the designated safeguarding lead.