“A cord of three strands is not easily broken”
Ecclesiastes 4:12

Weeting Primary School
Online Safety Policy



Written: October 2026
Review Date: October 2027

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and regional school board members.
- 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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories

Contact – being subjected to harmful online interaction with other users or generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes

Conduct – 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), including those generated using AI, 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 statutory safeguarding guidance, Keeping Children Safe in Education (2026) from the Department for Education (DfE) and its advice for schools on:

- Teaching online safety (2023)
- Meeting digital and technology standards (2026)
- Preventing and tackling bullying (2026)
- Relationships and sex education (RSE) and health education (2026)
- Searching, screening and confiscation (2023)
- Mobile phones in schools (2026)

It also refers to the DfE's guidance on protecting children from radicalisation (2026)
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Children's Wellbeing and Schools Act 2026 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 statutory requirements of the Early Years Foundation Stage.

3. Roles and responsibilities

3.1 The Regional School Board

The Regional School Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Regional School Board will ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (Designated Safeguarding Lead) and DDSL (Deputy Designated Safeguarding Lead) and any parental engagement.

The Regional School Board will make sure that 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 Regional School Board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Regional School Board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Regional School Board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Regional School Board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The Board will review the DfE's filtering and monitoring standards, and discuss with the Trust's IT Team 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 the school's safeguarding needs

All Regional School Board members will:

- Make sure 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 as detailed in the IT Acceptable Use policy.
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- Make sure 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).

3.2 The Headteacher

The Headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

They will make sure that there are robust cover arrangements in place for when the Designated Safeguarding

Lead is not on site or uncontactable to make sure safeguarding concerns are received, monitored and acted on without delay.

3.3 The Designated Safeguarding Leads and Deputy Designated Safeguarding Lead (DSLs and DDSL)

Details of the school's Designated Safeguarding Leads (DSL) and Deputy Designated Safeguarding Lead (DDSL) are displayed on posters around the school and in our Safeguarding and Child Protection policy.

The DSLs take lead responsibility for online safety in school, in particular:

- Making sure that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher and Regional School Board to review this policy annually and make sure 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 Trust's IT Team to make sure the appropriate systems and processes are in place.
- Working with the Headteacher, Trust's IT Team 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 Safeguarding and Child Protection and IT Acceptable Use policies.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Making sure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Behaviour policy.
- Updating and delivering staff training on online safety (Appendix 4 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services as necessary.
- Providing regular reports on online safety in school to the Regional School Board.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

3.4 Grace Schools IT Team

The Trust's IT Team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Making sure 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 regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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 as detailed in the school's IT Acceptable Use Policy, and making sure that pupils follow the school's terms on acceptable use (Appendices 1-3).
- Knowing that the DSL team is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes to the DSL team.
- Making a written request to the Headteacher if they need to bypass the filtering and monitoring systems for educational purposes. The Headteacher will then pass this request on to the Trust's IT Team for consideration.
- Working with the DSL team to make sure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour policy by reporting these directly to a member of the DSL team.
- 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' by reporting these directly to the DSL team.

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.
- Make sure that 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).

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

› Help and advice for parents/carers – Childnet

› Parents and carers resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy and the school's IT Acceptable Use policy and will be expected to agree and follow the terms in both (Appendix 3).

4. Educating pupils about online safety

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

The safe use of social media and the internet will also be covered in Personal, Social, Health and Economic (PSHE) education, where relevant. Teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. Appendix 6 of this policy contains an overview of the school's online safety curriculum.

In the **Early Years Foundation Stage** and **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.

- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.
- Be discerning in evaluating digital content.

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure.
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this.
- That there is a minimum age for joining social media sites, which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults.
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

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. This policy will also be shared with parents/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.
- The school's expectations in respect of appropriate use of AI by pupils.

If parents/carers 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 team. 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.

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 encourage them 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 as part of the Computing and Personal, Social, Health and Economic curriculum.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of annual and ongoing safeguarding Continuing Professional Development.

The school shares information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The Headteacher/DSL team 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 DSL team can carry out a search and confiscate any electronic device in line with the school's IT Acceptable Use policy. 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 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 whether 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 a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), including any image generated or altered by AI, they will not:

- View, copy, print, share, store, save, forward on, or ask a child to share or download, the image
- Delete the image or ask the pupil to delete the image
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any pupil involved

The staff member will remove the device and report the incident to the Headteacher and DSL team 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 (2023) 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 (2024).

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL team.

6.4 Artificial intelligence (AI)

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

Weeting Primary 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' or 'deep nudes', 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.

Weeting Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and Behaviour policies.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school and/or trust (Grace Schools) and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and Regional School board members are expected to follow the content of the IT Acceptable Use policy.

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 for pupils, volunteers and visitors in Appendices 1 to 3.

8. Pupils using mobile devices in school

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to

mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes. Children's mobile phones are signed in and out at the start and end of each day are stored in the school office during the school day.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by the headteacher. A risk assessment to show need will be completed and uploaded to Smart Log.

This does not include the use of laptops or tablets for learning. These devices should be used in accordance with our IT Acceptable Use policy.

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
- 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.
- Central IT team installation of anti-virus and anti-spyware software.
- Central IT team maintenance of operating systems.

Staff members must not use the device in any way that would violate the school's IT Acceptable Use policy. 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 Trust's IT team, Headteacher and/or DSL team.

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 Behaviour and IT Acceptable Use policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff Code of Conduct policy. 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 for staff and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages;

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, including images generated or altered by AI, especially around chat groups.
- Sharing of abusive images and pornography, including images generated or altered by AI, 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 DSLs and DDSL 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. Volunteers will receive appropriate training and updates, as applicable. More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

12. Monitoring arrangements

The DSLs log behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5. The log will be discussed as part of the fortnightly DSL meeting agenda.

This policy will be reviewed every year by the headteacher.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Behaviour policy
- Staff Code of Conduct policy
- Data protection policy and privacy notices
- Complaints policy
- IT Acceptable Use policy

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:	
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 and AI that a teacher or adult has told me or allowed me to use, and in a way in which a teacher or adult has told me I can use it › Tell my teacher immediately if: o I select a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends › Use school computers for schoolwork only › Be kind to others and not upset or be rude to them › Look after the school computers and devices 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 in a way that a teacher or adult has told me › Check with my teacher before I print anything › Log off or shut down a computer or other device 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 usernames and passwords safe and not share these with others › Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer › Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others › Always log off or shut down a computer when I've finished working on it **I will not:** › Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity › Open any attachments in emails, or follow any links in emails, without first checking with a teacher › Use any inappropriate language when communicating online, including in emails › Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate, including anything created using AI › 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 make sure it's switched off and handed in to my class teacher as required by school rules immediately upon entering the school › I understand that I am not permitted to look at, use, or have access to my device at any point during the school day – including during lessons, the time between lessons, breaktimes, and lunchtimes **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's 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 regarding a default ban on mobile devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, VOLUNTEERS AND VISITORS	
Name of volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: › Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) › Use them in any way that could harm the school's reputation › Access social networking sites or chat rooms › Use any improper language when communicating online, including in emails or other messaging services › Install any unauthorised software, or connect unauthorised hardware or devices to the school's network › Input, upload, or process any personal data of pupils, confidential safeguarding information, or sensitive school data into public or unvetted generative AI tools (such as public AI chatbots or image generators). I will make sure I am aware of approved AI tools for use in school and follow this at all times › 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 the purpose of 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 Headteacher and Designated Safeguarding Lead (DSL) know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (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/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 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**

Appendix 6 – Online Safety Curriculum
Cycle 1

	Autumn	Spring	Summer
Chestnut	**Online Relationships** I can recognise some ways in which the internet can be used to communicate.	**Privacy and Security** I can explain how some people may have devices in their homes connected to the internet and give examples.	**Copyright and Ownership** I can name my work so that others know it belongs to me.
Beech	**Online Relationships** I can give examples of how I use technology to communicate with people I know	**Managing Online Information** I can give simple examples of how to find information using digital technologies.	**Copyright and Ownership** I can save my work under a suitable title or name so that others know it belongs to me.
	Managing Online Information I can talk about how to use the internet as a way of finding information online.	**Online Reputation** I can identify ways that I can put information on the internet.	**Copyright and Ownership** I understand that work created by others does not belong to me even if I save a copy.
Elm	**Online Relationships** I can give examples of technology specific forms of communication	**Online Reputation** I can explain how to search for information about others online.	**Online Bullying** I can describe appropriate ways to behave towards other people online and why this is important.
	Online Reputation I can explain ways that some of the information about anyone on line could have been created, copied or shared by others.	**Privacy and Security** I can describe simple strategies for creating and keeping passwords private.	**Privacy and Security** I can describe effective ways people can manage passwords.
Oak	**Self Image and Identity** I can explain how identity online can be copied, modified or altered.	**Online Reputation** I can describe how to find out information about others by searching online.	**Online Bullying** I can describe ways people can be bullied through a range of media.
	Privacy and Security I can describe how connected devices can collect and share anyone's information with others. I can explain how many free apps or services may read and share private information with others.	**Managing Online Information** I can explain the benefits and limitations of using different types of search technologies. I can explain how some technology can limit the information I am presented with.	**Privacy and Security** I can explain what to do if a password is shared, lost or stolen. I can describe how and why people should keep their software and apps up to date.

Cycle 2

	Autumn	Spring	Summer
Chestnut	**Online Relationships** I can recognise some ways in which the internet can be used to communicate.	**Privacy and Security** I can explain how some people may have devices in their homes connected to the internet and give examples.	**Copyright and Ownership** I can name my work so that others know it belongs to me.
Beech	**Online Reputation** I can recognise that information can stay online and could be copied.	**Managing Online Information** I can use simple keywords in search engines	**Privacy and Security** I can explain how passwords are used to protect information, accounts and devices – session 1
		Managing Online Information I can demonstrate how to navigate a simple webpage to get information I need.	**Privacy and Security** I can explain how passwords are used to protect information, accounts and devices – session 2
Elm	**Online Reputation** I can search for information about an individual online and summarise the information found.	**Online Bullying** I can give examples of how bullying behaviour could appear online and how someone can get support.	**Privacy and Security** I can explain what a strong password is and demonstrate how to create one.
	Privacy and Security I can give reasons why someone should only share information with people they choose to and can trust. I can explain that if they are not sure or feel pressurised then they should tell a trusted adult.	**Copyright and Ownership** I can demonstrate how to make references to and acknowledge sources I have used from the internet.	**Online Reputation** I can describe ways that information about anyone online can be used by others to make judgements about an individual and why these may be incorrect.
Oak	**Copyright and Ownership** I can demonstrate the use of search tools to find and access online content which can be reused by others.	**Online Bullying** I can describe how to capture bullying content as evidence to share with others who can help me.	**Managing Online Information** I can explain what autocomplete is and how to choose the best suggestion.
	Privacy and Security I can describe strategies for keeping personal information private, depending on context.	**Online Reputation** I can explain strategies anyone can use to protect their "digital personality" and online reputation, including degrees of anonymity.	**Privacy and Security** I can describe simple ways to increase privacy on apps and services that provide privacy settings.