Online Safety Policy

and

Acceptable Use Agreement

Approved by:	WJS Full Governing Board	**Date:**	24.03.26
Last reviewed on:	Spring Term 2026		
Next review due by:	Spring Term 2027		

Contents

1. Aims

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, Whitehall Junior School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Protect and educate the whole school community in its safe and responsible use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate.
- Educate pupils about online safety as part of our curriculum.
- Train staff, 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.
- Educate parents/carers about online safety via our website, communications sent directly to them and during parents' evenings. We will also share clear procedures with them so they know how to raise concerns about online safety.
- Make all pupils, parents/carers, staff, volunteers and governors aware that they are expected to sign an agreement regarding the acceptable use of the internet in school, use of the school's IT systems and use of their mobile and smart technology.
- Set clear guidelines for the use of mobile phones and devices for the whole school community.
- Make sure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:
    1. Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present.
    2. Staff will not take pictures or recordings of pupils on their personal phones or cameras.
- Explain the sanctions we will use if a pupil is in breach of our policies on the acceptable use of the internet and mobile phones.
- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation.
- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described below) from the school's IT systems.
    - Carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks faced by our school community.

The 4 key categories of risk

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

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi- nudes and/or pornography), sharing other explicit images and online bullying.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- Cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation
- Protecting children from radicalisation.

The policy also refers to how our Online Safety curriculum will be taught, where guidance from the following documents have been taken into account:

- National Curriculum Computing programmes of study
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Education for a connected world

3. Roles and responsibilities

3.1 The Governing Board

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

The Governing Board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

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

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

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

The Governing Board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness.

The Governing Board 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 that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet. (Appendix 2)
- 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.

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's DSL [and deputy/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, IT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT provider, Turn IT On, and the school's IT Resources' Manager, to make sure the appropriate systems and processes are in place
- Working with the Headteacher, IT Resources' Manager 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 (see Appendix 4) with our school's safeguarding incident log, dealt with appropriately.
- 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 Governing Board.
- 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.

3.4 The SLT in partnership with our IT provider (Turn IT On)

The SLT/IT provider is responsible for (but not limited to):

- 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 IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's IT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged via our school safeguarding procedure and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School Behaviour policy.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for (but not limited to):

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (Appendix 2) and ensuring that pupils follow the school's rules on acceptable use (see 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 notifying the Headteacher.
- Following the correct procedures by contacting the Headteacher 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 (see Appendix 4) and dealt with appropriately in line with this policy
- Reporting incidents and concerns regarding online safety in a timely manner via the CPOMS reporting program. Ensuring they contact the DSL directly for urgent matters.

- Ensuring that any incidents of cyber-bullying are reported and 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'. Ensuring all incidents are recorded and reported via CPOMS.

3.6 Parents and carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Maintain awareness of current school policy and advice linked to online safety.
- Ensure their child adheres to school policy (Appendix 1) when borrowing a school device.

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
- Healthy relationships – Disrespect Nobody

Parents can also sign up to our National Online Safety account for videos and information sheets about particular apps and concerns by using our school link:
https://nationalonlinesafety.com/enrol/whitehall-junior-school

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. Our pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online

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

All schools have to teach:

- Relationships education and health education in primary schools

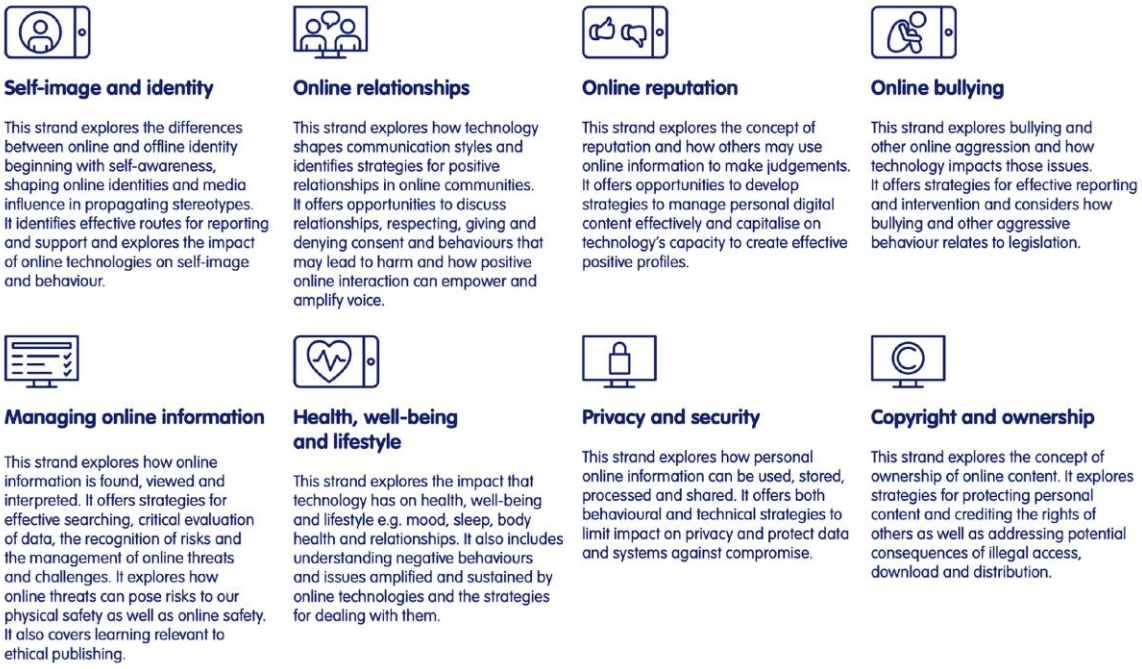
The safe use of social media and the internet will also be covered in other subjects where relevant.

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

Online safety will be taught to children through:

- Bespoke assemblies
- Circle time
- PSHE and RHSE lessons
- Computing lessons

Our school will teach online safety, referring to the 'Education for a Connected World' DfE guidance, ensuring that we cover each strand with age-appropriate knowledge across the children's KS2 curriculum.



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.

Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

4

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in newsletters or other communications, and in information via our website.

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 DSL.

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.

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

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

The school also sends information/leaflets on cyber-bullying to parents/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 **Anti-Bullying Policy**. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of our school SLT or Safeguarding Team 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 Deputy Headteacher (or Deputy Designated Safeguarding Lead)

- 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/ DSL or other members 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 (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- 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.

Whitehall Junior 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.

Whitehall Junior School will treat any use of AI to bully pupils in line with our Anti-Bullying/Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

Staff must thoroughly check and edit any information they generate from AI before including it in school planning.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to adhere to the school's acceptable use agreements (Appendix 1 and 2) on all school devices.

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

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

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

8. Pupils having mobile devices in school

If a pupil needs to bring a mobile phone to school, this must be agreed with the parent and class teacher. This should only be done if necessary for traveling arrangements and a log is kept of pupils with permission to travel independently.

The children may not store their phone on their person or in their bag or coat. Mobile phones must be turned off and handed to the class teacher at the start of the day and will be returned at the end of the school day. Children will not be permitted to have access to their phone throughout the school day.

The school cannot take any responsibility for loss or damage to a phone or electronic device brought into school.

Any breach of this acceptable use agreement by a pupil may lead to disciplinary action in line with the behaviour policy.

Should the school have reason for concern about any material brought to our attention on a child's device, the DSL will take the appropriate action following government guidelines (Education and Inspections Act 2006).

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 eight 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 is locked 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 from the school network.
- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.
- Work devices must be used solely for work activities.
- Devices may not be used to access inappropriate content or information that violates the staff code of conduct.

If staff have any concerns over the security of their device, they must seek advice from the school IT provider.

10. Pupils using devices loaned to them by the school at home

In some instances where children need to learn from home, a device may be loaned to a child to support them with their online education. This would have to be arranged with the Headteacher and is agreed on a case-by-case basis.

Children must follow the device rules (Appendix 1).

Using the device appropriately

The device should only be used by the child it has been loaned to for the purposes of study. It cannot be used for personal activities such as online gaming, social media and personal emails.

Looking after the device

Children and families must ensure they are using the device respectfully, reducing the risk of damage by keeping it away from water and dirt, and out of reach of pets and younger children.

Maintaining security of the device

The device will be set with a password specific to your child, this should not be shared. Parents should keep the device in a safe place whilst a child is not studying. The school must be made aware if there are any technical issues with the computer and it should be returned to the school promptly.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The individual circumstances, nature and seriousness of the specific incident will be taken into account and the response will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device, where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and 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. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.
All incidents must be recorded on the CPOMS software under category 'Online Safety' so that the DSL may review these.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the Governing Board. The review (such as the one available here on 360 safe) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

14. Training

All new staff members will receive training, as part of their safeguarding 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).

Teaching staff will receive further training concerning online safety within the curriculum.

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:
    1. Abusive, threatening, harassing and misogynistic messages
    2. Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    3. 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
- The 4 risk categories of online safety are, 'content, contact, conduct and commerce' and what each of these risk categories entails.

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 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 and updates, as applicable.

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

Appendix 1- Acceptable use policy for children

Device Rules
(iPads, laptops, netbooks, computers)

How I use devices:

1) I will only use the school device for schoolwork as assigned by my teacher.
2) I will ask permission before choosing a new website.
3) I will not use school equipment for any form of social media and online messaging.
4) I will not share passwords to my accounts with others.
5) I will not attempt to login to someone else's account.
6) I will tell my teacher if somebody tries to contact me or if something inappropriate appears on my screen.
7) I will not make any edits to computer settings or attempt to download new programs.

How I treat devices:

1) I will look after school equipment, treating it with care and consideration.
2) I will keep food and drink away from devices.
3) I will alert my teacher immediately to any faults or damage on devices.
4) When borrowing school devices, I understand that the device is for my schoolwork only and must not be shared.

Appendix 2 – Acceptable use policy for 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 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 ● Share my password with others or log in to the school's network using someone else's details ● Take photographs of pupils if I am a governor/volunteer/visitor (teachers may do so for educational purposes if permission has been sought and only using school devices) ● 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 designated safeguarding lead (DSL) and ICT manager 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 (staff member/governor/volunteer/visitor):	**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?	