

Online Safety Policy

2025-2026

Monitoring and review

This policy will be reviewed annually by the Proprietors to assess its effectiveness. The policy will be promoted and implemented throughout the school.

Staff With Responsibility For Policy:		Jacob Hardman	
Date Established:	Spring Term 2021	Review Cycle:	Every One Years

Document Control & Review			
Date:	Action:	Changes Made:	By:
07.02.21	Created	Policy created and sent out for consultation	
09.03.23	Reviewed		SJ
29.08.23	Reviewed	Updated the cyber-bullying section	
10.01.24		Updated the artificial intelligence (AI) section (6.4) to include a reference to deep fake pornography.	JH
07.10.24	Reviewed		
11.03.25	Reviewed	Updated visitor access protocol	SJ
11.09.25	Reviewed	Reviewed – no major changes - online safety incident report log included in Appendix 5	JH
09.01.26	Amended	Amended to ensure expectations around teaching, learning and supervision are clear.	SJ

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	4
4. Filtering and Monitoring Systems	7
5. Educating Students about online safety	9
6. Teaching and Learning – Staff Supervision and Expectations	9
7. Educating parents/carers about online safety	10
8. Cyber-bullying	10
9 Acceptable use of the internet in school.....	13
10. Students using mobile devices in school.....	13
11. Staff using work devices outside school.....	13
12. How the school will respond to issues of misuse	14
13. Training	14
14. Monitoring arrangements	15
15. Links with other policies	15
Appendix 1: Acceptable Use of the School's ICT Systems and Internet: Agreement for Pupils and Parents/Carers	16
Appendix 2: Acceptable Use of the School's ICT Systems and Internet: Agreement for Staff, Proprietors, Volunteers and Visitors	17
Appendix 3: online safety training needs – self audit for staff	18
Appendix 4: Request to Block / Unblock Website.....	19
Appendix 5: Online Safety Incident Report Log	19

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and proprietors.
- Identify and support groups of students 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 Principals 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 Students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Proprietors

The proprietors have overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

3.2 The Principal

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

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

The Principal must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. They 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 in making sure an appropriate level of security protection procedures, such as filtering, monitoring and parental controls on

school devices and networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material without unreasonably impacting teaching and learning;

- Ensuring effective monitoring strategies are in place that meet their safeguarding needs.
- Ensuring that online safety is a running and interrelated theme across the school and where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students 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.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly to ensure that potentially dangerous sites are blocked, where possible, preventing the downloading of potentially dangerous files
- Conducting a full security check and monitoring the school's ICT systems on a half termly basis
- Ensuring that any online safety incidents are logged using CPoms and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our safeguarding policy, as well as relevant job descriptions.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal and Proprietors to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Working with the Principal to make sure the appropriate systems and processes are in place
- Working with the Principal 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 using CPoms and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- 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 - (Appendix 3 contains a self-audit for staff on online safety training needs)

3.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that Students follow the school's terms on acceptable use.
- Being aware of their responsibility in the filtering and monitoring of online access including following the correct procedures for making a request if they need to bypass the filtering and monitoring systems for educational purposes – Section 4.
- Ensuring that any concerns online safety incidents, cyber-bullying, sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here' are reported and dealt with appropriately in line with the school behaviour policy
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Principal 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 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](#)
- Hot topics – [Childnet](#)
- Parent resource sheet – [Childnet](#)
- <https://www.internetmatters.org/>

3.6 Visitors and Outside Agencies

Visitors to the school will not ordinarily be given access to the school internet using non-school owned devices. This is to ensure the integrity of our network and reduce risks associated with encryption, VPNs and other forms of privately restricted portals and where SSL inspection of devices is not possible. Where possible guest access will be provided to an alternative internet access provider.

4. Filtering and Monitoring Systems

Schools in England and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." Ofsted concluded as far back as 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

In pursuing a route of good management of online access we ensure that:

- Providers of internet access to the school are IWF members and use IWF services to block access to illegal Child Sexual Abuse Material (CSAM). Adult content and websites using offensive language are also filtered at source.
- Filtering at source of known websites containing harmful content using parental controls.
- Access to social media main platforms blocked at source using parental controls.
- Filtering is constantly informed by active supervision and staff report any incidents whereby (Appendix 4):
 - Someone has accessed or tried to access unsuitable content
 - There's a failure in the software or an abuse of the system
 - Someone is using abbreviations or misspellings to access restricted material
 - There are unreasonable restrictions that affect teaching or admin tasks
 - You're teaching a topic that could create unusual activity on the filtering logs

"I saw one child search for 'mia content'. While this might sound like they're searching for a girl's name, maybe a YouTuber called Mia, I knew this was also code for **pro-bulimia content**. I reported this to the designated safeguarding lead who was able to follow up with the child. They had a deeper conversation with the child about eating disorders to see whether she needed further support."

However, it is important to recognise that no filtering or monitoring systems can be 100% effective in preventing or capturing every concern and need to be supported with good teaching and learning practice and effective supervision. As such, filtering systems should be recognised as one of the tools used to support and inform the broader safeguarding provision in settings. The most important tool in keeping students safe online is the effective supervision and the eyes and ears of all staff.

In addition to the filtering systems described:

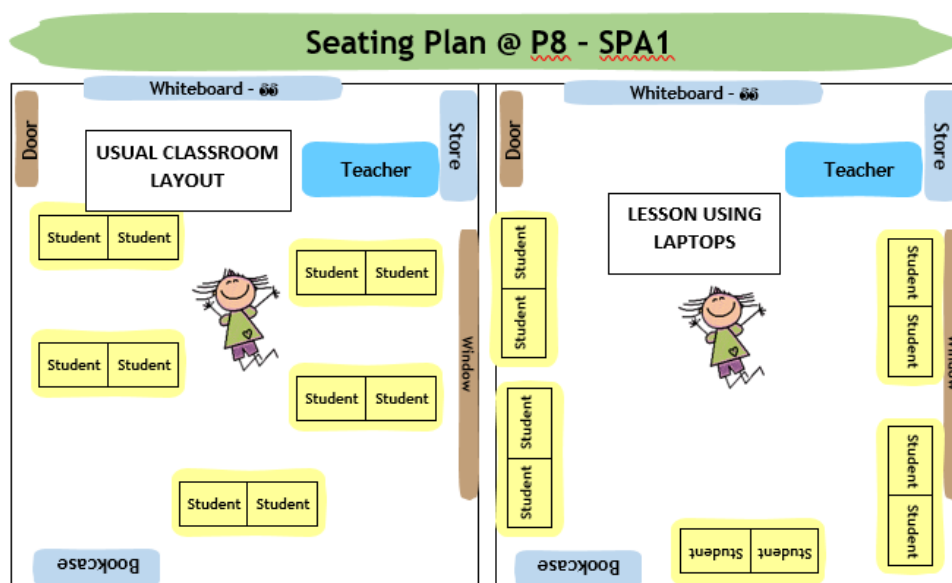
- Students do not have unsupervised access to the internet in school.
- All staff are aware of how students are using devices to access the internet.
- Classroom organisation ensures visual supervision (all laptop screens facing centre of room and visible to teaching staff, regular visual sweeps, regular checking for hidden tabs)

5. Teaching and Learning – Staff Supervision and Expectations

One of the most powerful and effective protection tools in keeping children safe online is in the effective supervision and clear, consistent expectations of online behaviour.

Where the internet is being used, or where laptops or other devices with internet access are being used in lessons then:

- Desks are organised so that laptop screens are facing inwards towards the centre of the room. This may mean reorganising classrooms in preparation for lesson, or in some cases, part way through a lesson. The school health and safety policy also specifies that desks should be against walls to prevent trailing leads from causing trip hazards. The two diagrams below show how a classroom may need to be reorganised when laptops are being used.



- Students have clear and specific direction as the purpose of any online learning. This could be by providing a list of websites to be visited. Students should **never** just be given free rein or vague direction just to “carry out research”.
- Students are **never** allowed to access **music** or **video streaming** sites such as **YouTube** or similar in lessons.
- Students **should not** usually be given headphones whilst online as this makes it extremely difficult for staff to monitor what is being accessed or listened to. If headphones are given this needs to be for a specific time limited purpose under close supervision.
- Due to the impact on internet speeds access to sites streaming video or music content is not allowed.
- Students should never be given independent access to a staff laptop.

6. Educating Students about online safety

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

In **KS3**, Students 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

Students in **KS4** 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 secondary school**, Students 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 some Students with SEND.

7. 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 or social media platforms. This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

8. Cyber-bullying

8.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups.

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

All staff, proprietors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

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 behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, 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.

8.3 Examining electronic devices

The Principal, and any member of staff authorised to do so by the Principal can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, 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 students and staff. If the search is not urgent, they will seek advice from the Principal.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student'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 staff member in conjunction with the DSL / Principal 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 student 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 students 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](#)

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

8.4 Artificial intelligence (AI)

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

Our school recognises that AI has many uses to help students 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.

Our school will treat any use of AI to bully students in line with our anti-bullying 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.

9. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and proprietors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 2). 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 students, staff, volunteers, proprietors 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.

10. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during the school day or inside the school building. They can use their mobile devices during break and lunchtimes in the school courtyard.:

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

11. 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 the ICT manager.

12. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

13. Training

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

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

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, 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 Students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and ICT Manager 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.

Proprietors 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.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPoms. An incident report log can be found in appendix 5.

This policy will be reviewed every year. At every review, the policy will be shared with the proprietors. The review will be supported by an annual risk assessment (such as the one available [here](#)) that considers and reflects the risks Students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Links with other policies

This online safety policy is linked to our:

- 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 of the School's ICT Systems and Internet: Agreement for Pupils and Parents/Carers

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

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carers
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carers, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will hand it in to the office to be locked away whilst I am in the building and only use it in the courtyard at break and lunchtimes.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carers' agreement: I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

Appendix 2: Acceptable Use of the School's ICT Systems and Internet: Agreement for Staff, Proprietors, Volunteers and Visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, PROPRIETORS, VOLUNTEERS AND VISITORS

Name of staff member/ proprietors/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for 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 which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/ proprietors/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, proprietors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Request to Block / Unblock Website

REQUEST TO BLOCK/UNBLOCK A WEBSITE

Phoenix Learning Communities employs filtering on all devices with internet access, including all wireless connections. However, we are aware that no filtering system will ever be 100% effective. Filters can sometimes inadvertently block sites that are useful in aiding teaching and learning or alternatively fail to block sites that may be considered objectionable or potentially harmful.

If you believe a site has been unfairly blocked, or that an unblocked site violates the company's online safety policy, please fill out this form and return it to the office email address for consideration. The site will be critically evaluated within 48 hours. Site(s) which violate the Company Internet Acceptable Use Policies or other policies will be added to a company-specific blacklist and will be blocked from further access. Sites which are not found to violate any policies will be added to a company-specific whitelist.

WEBSITE ADDRESS:

I WOULD LIKE THIS SITE TO BE: BLOCKED: ☐ UNBLOCKED: ☐
--

REASON FOR YOUR REQUEST:

NAME:	 	DATE:	
--------------	----------	--------------	----------

DECISIONS AND JUSTIFICATIONS:

NAME:	 	DATE:	
--------------	----------	--------------	----------

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