



Blatchington Mill School

Online Safeguarding Policy

Date Policy Created:	February 2020
Date of last amendment:	September 2026
Next review:	September 2028



Contents

1. Aims	3
2. Legislation and guidance	3
2.1 Department for Education	3
2.2 Education Act	4
2.3 Other relevant legislation	4
3. Roles and responsibilities	4
3.1 The governing board	4
3.2 The headteacher	5
3.3 The designated safeguarding lead (DSL)	5
3.4 The network services systems manager	6
3.5 All staff and volunteers	6
3.6 Families	7
3.7 Visitors and members of the community	7
4. Educating students about online safety	7
4.1 Students will be taught about online safety as part of the curriculum	7
4.2 Students will be taught practical cyber security skills	9
5. Educating parents/carers about online safety	9
6. Cyber-bullying	9
6.1 Definition	9
6.2 Preventing and addressing cyber-bullying	10
6.3 Examining electronic devices	10
6.4 Artificial intelligence (AI)	11
7. Acceptable use of the internet in school	12
8. Social networks	12
8.1 Social media	12
9. Students using mobile devices in school	13
10. Staff using work devices outside school	13
11. How the school will respond to issues of misuse	13
12. Training for staff, governors and volunteers	14
13. Monitoring arrangements	14
14. SEND	15
14.1 Education and training	15
14.2 Reporting concerns	15
15. Links with other policies	15
16. Online Safeguarding Contacts and References	15
Appendix 1: Acceptable use policy for the school's ICT systems and internet	17
Appendix 2: online safety training needs – self-audit for staff	18



1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- 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, 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

2.1 Department for Education

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

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

It also refers to the DfE's guidance on [protecting children from radicalisation](#).



2.2 Education Act

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 students' 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.

2.3 Other relevant legislation

- [Data Protection Act 2018](#) and General Data Protection Regulation (GDPR) - Sets out how personal data is to be protected and only used for the intended purpose when shared.
- [The Computer Misuse Act](#) - Makes it an offence to:
 - access computer material without permission; e.g. looking at someone else's files
 - access computer material without permission and with intent to commit criminal offences; e.g. hacking into your bank's computer and increasing the money in your own account
 - alter computer data without permission; e.g. writing a virus to destroy someone else's data
- [Sexual Offences Act 2003](#) - Defines and determines the severity of all sexual offences in the UK, including the offence of sexual grooming.
- [Malicious Communications Act 1988](#) - Makes it an offence to send a communication with the intention of causing distress or anxiety.
- [Communications Act 2003 Section 127](#) - Makes it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character.

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 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 (and deputies) and any parental engagement.

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 requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches students how to keep themselves and others safe, including online.

The governing 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 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 the school's safeguarding needs

The governor who oversees online safety is Mr Andrew Fozard.

All governors 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 (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college 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 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

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 for when the DSL is unavailable due to illness, leave or other circumstances – for example, a confidential shared mailbox to make sure safeguarding concerns are received, monitored and acted on without delay.

3.3 The designated safeguarding lead (DSL)

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

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing 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
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the network services systems manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, network services systems 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



- 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 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 if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks students face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The network services systems manager

The network services systems manager 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 students 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
- 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 dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that students follow the school's terms on acceptable use (appendices 1 and 2)
- 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 reporting them to the DSL and Network Services, as well as the relevant Year Office (if any students are involved with the system failure).



- Following the correct procedures by requesting access from Network Services if they need to bypass the filtering and monitoring systems for educational purposes
- 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
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Families

We support and encourage a partnership approach with families. 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)

Families 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 ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating students about online safety

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

All schools have to teach:

- Relationships and sex education and health education in secondary schools

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:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online



- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Students should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and/or may post things which aren't real/have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Students should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Students should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Students should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Students should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Students should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Students should be taught where to go for advice and support about something they have seen online. Students should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect students who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion



- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

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.

4.2 Students will be taught practical cyber security skills

All students 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

Students 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 supports raising families' awareness of internet safety through this policy, in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Parents/carers can request further information on:

- the school systems used to filter and monitor online use
 - Smoothwall, a web content filtering, safeguarding and internet security platform used in schools, and
 - SENSO, a software package for network, classroom, safeguarding and asset management
- 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
- Any queries or concerns in relation to online safety or this policy can be raised with any member of staff, but ideally these should be raised with the students' Year Office in the first instance.

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 1 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 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 encourage them 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. This will be done through a combination of work in personal, social, health education (PSHE), form tutor time activities, year group assemblies, as well as in computer science lessons.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying in other subjects where appropriate.

All staff, governors and volunteers (where appropriate) can access training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11).

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.

Families can learn more about general E Safety, including cyberbullying, so they are aware of the signs, how to report it and how they can support children who may be affected through organisations and websites listed in Section 15.

6.3 Examining electronic devices

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

- 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

Members of SLT and Year Office teams 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 DSL and headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding 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 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), 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 student to delete the image
- Ask the student(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 student(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any student involved

The staff member will 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](#).

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

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](#)
- Our behaviour policy/searches and confiscation policy

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

6.4 Artificial intelligence (AI)

Generative 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 Gemini.

Blatchington Mill 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' 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.

Blatchington Mill School will treat any use of AI to bully students 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 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, students and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy



7. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and governors are expected to confirm they have read an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1). 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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Social networks

All members of the school community should bear in mind that the information they share through social networking applications, even if they are on private spaces, may be subject to copyright, safeguarding and data protection legislation. Everyone is to operate in line with the relevant school policies on equalities, harassment, child protection, safer recruitment, and online safety and ICT acceptable use, whether during school hours or otherwise.

8.1 Social media

For the purposes of this document, 'social media' is considered to include all technologies that allow individuals to communicate and share information (including photos and video). Examples include: Facebook, Snapchat, Instagram, WhatsApp, X, YouTube, TikTok, KIK, Flickr, Tumblr, forums, bulletin boards, multiplayer online gaming, chatrooms, Instant Messenger, video conferencing platforms, and many others.

- The school will block/filter access to social networking and newsgroup sites other than those approved by the school for use in school.
- Official school social media posts, blogs or wikis will be password protected and run within the school.
- We would ask that everyone in our school community is respectful of others and posts reflect the values and ethos of the school.
- Students are advised:
 - never to give out personal details which may identify them and/or their location. Examples include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends, specific interests and clubs etc.
 - not to place personal photos on social network spaces without due consideration and regard to background detail in a photograph which could identify the student or location (e.g. house number, street name or school).
 - on security, and encouraged to set strong passwords, to deny access to unknown individuals and instructed how to block unwanted communications.
 - to only invite or accept known friends and deny access to all others.
 - that allowing access to a friend on their social network space could allow access to friends of that friend, who would be unknown to the student.
 - not to publish specific and detailed private thoughts.
- Staff are advised not to:
 - run social network spaces for student use on a personal basis.
 - befriend, seek to befriend, or communicate with students on any social networking site or outside the official school system.



Staff members should also read our staff Code of Conduct and the Social Networking Policy for Employees of Brighton & Hove City Council as well as staff updates as appropriate (for example through staff emails and staff meetings).

9. Students using mobile devices in school

In line with statutory guidance, our school is a mobile phone-free environment by default. Students 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.

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.

Where there is an arrangement by exception, 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 a sanction in line with the school behaviour policy, which may result in the confiscation of their device. Please see our behaviour policy for further details

10. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager
- 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 promptly 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 3.

Work devices must be used solely for work activities.

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

11. 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 this and our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training for staff, governors 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 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 DDSs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The DSL, DDSs and Year Office teams log behaviour and safeguarding issues related to online safety on CPOMS (Child Protection Online Monitoring System).

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with the governing board. 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.



14. SEND

14.1 Education and training

When teaching about online safety, learners with special educational needs and/or disabilities (SEND) may need:

- complex online safety issues to be broken down and explained in other ways
- to explore issues in a variety of contexts and approaches (e.g. cause and effect)
- more examples of safe and unsafe practices
- extra reinforcement and repetition of key safety messages
- differentiated teaching resources and materials
- more engagement with families, as they play a vital role in supporting children to learn how to be safe online

14.2 Reporting concerns

Learners with SEND may require a range of methods to enable them to report concerns and seek support. Examples include:

- Non-verbal learners may require a messaging or sound system on their devices to help them to get adult attention
- Learners may have 1-2-1 workers or trusted adults that they prefer to speak to who will be able to support the DSL in communicating with the learner

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- AI policy

16. Online Safeguarding Contacts and References

- General Advice on Staying Safe Online
 - Childline - <http://www.childline.org.uk/>
 - Internet Matters - <http://www.internetmatters.org/>
 - UK Safer Internet Centre - <https://www.saferinternet.org.uk/> (Helpline for professionals)
 - NSPCC - <https://www.nspcc.org.uk/keeping-children-safe/online-safety>
 - Think U Know website - <http://www.thinkuknow.co.uk/>
 - Digital Parenting - <https://parentzone.org.uk/>
- Reporting
 - Child Exploitation & Online Protection Centre - <https://www.ceop.police.uk/safety-centre/>



- Childnet International - <http://www.childnet.com>
- Internet Watch Foundation - <http://www.iwf.org.uk/> (Anonymously)
- Remove Nude or Sexual Contents
 - Internet Watch Foundation - <http://www.iwf.org.uk/> (Anonymously)
 - Childline - <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/>
- Cyberbullying Guidance
 - Childnet - <https://www.childnet.com/resources/cyberbullying-guidance-for-schools/>



Appendix 1: Acceptable use policy for the school's ICT systems and internet

The Acceptable Use Policy (AUP) is found on school Microsoft desktops in the form of popups every seven days. If any user (including students, staff, governors, visitors, etc) does not accept the conditions, the system will not open for the individual to use.

The terms of the Acceptable Use Policy are as follows:

- All users, including students and staff, have access to the school ICT systems on the understanding that they accept the terms laid out in this 'Acceptable Use Policy for the School's ICT Systems' document.
- Access must only be made via your authorised login and password. Your password must not be made available to any other person.
- All internet use should be appropriate to staff professional activity or student's education and learning.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden.
- Sites and materials accessed must be appropriate to work in school.
- Users are responsible for email that they send and for the contacts they make that may result in email being received.
- Professional levels of language and content should be applied to all forms of digital communications both internal and external.
- Copyright of materials and intellectual property rights must be respected at all times.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Students' use of chat rooms, or any other interactive message board is forbidden unless specifically directed by a member of staff.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety is unacceptable.
- Users must ensure they are aware of their own e-safety at all times. The school has published an 'Online Safeguarding Policy' document which is available to any user from the school website.
- Users must not bring the school, or any members of the school community, into disrespect by publishing any form of defamatory material on the internet which is then available for viewing by others.
- The use of mobile devices is only allowed in strict accordance with the terms of our behaviour policy and staff code of conduct.
- The school may check any user's computer files, monitor the internet sites they visit, or inspect their email at any time and without their knowledge.
- If you are unsure of any rules, please seek advice from the Network Services Office.



Appendix 2: 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?	