



Reach Schools

Online Safety Policy

Document Control Table	
Title	Online Safety Policy
Category	Student
Owner	Trust Designated Safeguarding Lead
Date approved	2nd July 2026
Approved by	Board of Trustees
Date of next review	September 27
Updates/revisions	July 2026 - Pupils and parents complete acceptance of ICT Acceptable use via the general information form
Schools to note: This is a Reach template, but it must be checked for local context and procedures before being submitted for approval. At Reach Schools, we believe that online safety (e-safety) is an essential element of safeguarding students and adults in the digital world, when using technology such as computers, mobile phones or games consoles. We identify that the Internet and information communication technologies are an important part of everyday life so students must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.	



Contents

1. Introduction	2
2. Aims	2
3. Legislation and Guidance	3
4. Roles and responsibilities	4
3.1 The Board of Trustees and LGB	4
3.2 The Co-headteachers	6
3.3 The Designated Safeguarding Lead	6
3.4 ICT Managed Services	7
3.5 Director of Operations	8
3.6 All staff and volunteers	9
3.7 Families	10
3.8 Visitors and members of the community	10
5. Educating students about online safety	10
4.2 Pupils will be taught practical cyber security skills	15
6. Educating families about online safety	16
7. Cyber-bullying	16
7.1 Definition	16
7.2 Preventing and addressing cyber-bullying	17
7.3 Examining electronic devices	18
8. Artificial intelligence (AI)	20
9. Acceptable use of the internet in school	20
10. Students using mobile devices in school	21
11. Staff using work devices outside school	21
12. How the school will respond to issues of misuse	22
13. Training	23
14. Monitoring arrangements	24
15. Links with other policies	25
Appendix 1: acceptable use agreement (governors, trustees)	26



**Reach
Schools**
CHOICE & OPPORTUNITY
FOR EVERY CHILD

1. Introduction

The purpose of this policy is to ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices to provide staff and volunteers with the overarching principles that guide our approach to online safety. This policy also ensures that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. This policy applies to all staff, volunteers, children and young people and anyone involved at Reach Schools.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, trustees 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'); and
- 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

3. 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](#) and [cyber-bullying: advice for headteachers and school staff](#)

[Relationships and sex education](#)

[Searching, screening and confiscation](#)



**Reach
Schools**
CHOICE & OPPORTUNITY
FOR EVERY CHILD

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.

The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

4. Roles and responsibilities

3.1 The Board of Trustees and LGB

The Board of Trustees has overall responsibility for monitoring this policy and holding the co-headteachers to account for its implementation.

Within the school, the Local Governing Body (LGB) 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 LGB 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 LGB 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 Board of Trustees and LGB should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Board of Trustees will ensure that the schools within Reach Schools have appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The 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 trust in meeting those 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; and
- Having effective monitoring strategies in place that meet their safeguarding needs.

The safeguarding link governor will act in a link role in relation to online safety and abidance by this policy.

All trustees and LGB members will:

- Ensure they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of Reach School's ICT systems and the internet (appendix 1);
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures; and
- Ensure 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 Co-headteachers

The Co-headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the schools.

3.3 The Designated Safeguarding Lead

Details of our 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 co-headteachers in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the co-headteacher to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks;
- Working with the ICT manager to make sure the appropriate systems and processes are in place;
- Working with the co-headteacher, ICT 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 and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the headteacher and/or LGB;
- Undertaking annual risk assessments that consider and reflect the risks children face; and
- 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 ICT Managed Services

Gridserve are responsible for:

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



- Antivirus Protection: Sophos antivirus is deployed across systems and is kept fully up to date to ensure protection against the latest threats.
- Server Updates: Servers are maintained and updated on a regular 6-week cycle to ensure security patches and system stability.
- Connectivity Management: Leased lines are managed externally through LGFL, providing secure and reliable internet connectivity.
- System Monitoring: Senso is in place and continuously monitors systems, providing real-time safeguarding and activity oversight.
- Google Workspace: Google Workspace services are updated automatically via Google's platform, ensuring the latest security and functionality are always in place.

This combination of proactive maintenance, automated updates, and continuous monitoring ensures that the school's ICT environment remains secure, compliant, and well-managed.

- 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 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 Director of Operations

- The operations manager is responsible for overseeing Gridserve;
- Support the DSL in the new KCSIE 2026 filtering and monitoring requirements; and



- Be responsible for any concerns pertaining to staff members online usage and violations, all issues will be logged on Staffsafe

3.6 All staff and volunteers

- 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 (which is within the staff handbook), and making sure that pupils follow the school's terms on acceptable use (which is shared via the general information form)
- 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 speaking to the DSL and speaking to our Director of People Following the correct procedures by speaking to Gridserve and the DSL 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 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.



3.7 Families

Families are expected to:

- Notify a member of staff or the co-headteacher of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2); and
- Families 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 International](#)
 - Families resource sheet – [Childnet International](#)
 - Healthy relationships – [Disrespect Nobody](#)

3.8 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.

5. Educating students about online safety

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

All schools have to teach:

[Relationships education and health education](#) in primary schools

[Relationships and sex education and health education](#) in secondary schools



**Reach
Schools**
CHOICE & OPPORTUNITY
FOR EVERY CHILD

In Key Stage 1, students will be taught to:

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

Students in Key Stage 2 will be taught to:

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

By the end of primary school, students will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults



- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

In Key Stage 3, 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; and
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in Key Stage 4 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, pupils 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. Pupils 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. Pupils 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. Pupils 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. Pupils 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. Pupils 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. Pupils 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



**Reach
Schools**
CHOICE & OPPORTUNITY
FOR EVERY CHILD

- 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. Pupils should be taught where to go for advice and support about something they have seen online. Pupils 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 pupils 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 pupils with SEND.

4.2 Pupils will be taught practical cyber security skills

The following items come from the DfE's [non-statutory cyber security standards for schools and colleges](#).

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

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



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

6. Educating families about online safety

The school will raise families' awareness of internet safety in letters, newsletters or other communications home. This policy will also be shared with families.

Online safety will also be covered during families' evenings/sessions. The school will let families know:

- What systems the school uses to filter and monitor online use; and
- 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 families have any queries or concerns in relation to online safety, these should be raised in the first instance with the Co- headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

7.1 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's behaviour and anti-bullying policies).



7.2 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.

We 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 tutors 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 Team Reach education, and other subjects where appropriate.

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

We also send information on cyber-bullying to families so that 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 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.



7.3 Examining electronic devices

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

- Poses a risk to staff or 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 Co-headteacher or DSL;
- 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 students co-operation; and

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 / co-headteacher / 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 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 families 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:



**Reach
Schools**
CHOICE & OPPORTUNITY
FOR EVERY CHILD

- 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 students' electronic devices will be dealt with through the school complaints procedure.

8. Artificial intelligence (AI)

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

Reach Schools 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.

Reach Schools will treat any use of AI to bully students in line with our behaviour policy.

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

9. Acceptable use of the internet in school

All students, families, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3).



Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by students, 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 to 3.

10. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to have them out on the school premises except for sixth form who may have them at break and lunch. If a student is seen or heard using their mobile devices then a consequence will be issued. Please see the schools behaviour policy for more information.

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 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 – always install the latest updates; and
- Staff members must not use the device in any way which would violate the school's terms of acceptable use..

Work devices must be used solely for work activities.

Please see the ICT acceptable use policy in the staff handbook.

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



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 as a part of their safeguarding training.

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 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, 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



**Reach
Schools**
CHOICE & OPPORTUNITY
FOR EVERY CHILD

- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- 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 deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding policy.

14. Monitoring arrangements

Senso is our monitoring system.

Senso flags users who may be vulnerable or at-risk and users who may pose a risk to others, as well as any inappropriate or harmful behavior, this is for both students and staff. Senso will immediately alert the operations manager and the DSL via email should any urgent or critical violations be triggered.

Any urgent or critical violations will be treated as a purple and our safeguarding policy will be followed.

The operations manager will oversee Staff violations and all positive concerns will be logged on Staffsafe and as well as on the Senso Platform. Any false positive will be recorded on the Senso Platform.

The DSL will oversee student violations and all positive concerns will be logged on CPOMs and as well as on the Senso Platform. Any false positive will be recorded on the Senso Platform.

Senso provides us with key reports which we will use to understand trends and behavior and inform the basis of staff training and student Team Reach lessons.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Board of Trustees. The review will be supported by an annual risk assessment 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:

- Child protection and safeguarding policy
- Behaviour policy
- Complaints procedure
- ICT and internet acceptable use policy



Appendix 1: acceptable use agreement (governors, trustees)

Acceptable use of the school's ICT systems and internet: agreement for governors and trustees

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 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 students without checking with teachers first
- Share confidential information about the school, its students 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) know if a student 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 students in my care do so too.

Signed (staff member/governor/volunteer/visitor)

Date:



**Reach
Schools**

CHOICE & OPPORTUNITY
FOR EVERY CHILD