The 3-18 Education Trust

Online Safety Policy

‘Every individual is in a great school.’

Approved:	**Spring Term 2024**
Review:	**Spring Term 2026**

www.3-18education.co.uk

Our Mission

To celebrate the diverse nature, culture and identity of our individual schools, whilst collaborating and enjoying the benefit of the team.

Our Values

Compassionate

To show care and understanding towards others.

Accomplished

To provide high quality education and training for all.

Resilient

To be solution focused and able to intelligently manage challenges.

The 3-18 Education Trust
Bowbrook Primary School
Squinter Pip Way
Bowbrook
Shrewsbury
SY5 8PY

Company Number: 08064698

Policy Monitoring and Review

Monitoring

The Chief Executive Officer will monitor the outcomes and impact of this policy on an annual basis.

Review

Member of Staff Responsible	Deputy Chief Executive Officer
Relevant Guidance/Advice/Legal Reference	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 schoolshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying and cyber-bullying: advice for headteachers 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 pupils' electronic devices where they believe there is a 'good reason' to do so.
Policy Adopted By	Board of Trustees
Consultation	Local Governing Bodies
Date of Policy	Spring Term 2024
Review Period	2 Years
Date of Next Review	Spring Term 2026

Contents

1. Introduction

1.1. This Online Safety Policy outlines the commitment of The 3-18 Education Trust (Trust) to safeguard members of its school community (including members, trustees, local governors, staff, volunteers, pupils, parents and carers, visitors, community users) online in accordance with statutory guidance and best practice.

1.2. This Policy applies to all members of the school community who have access to and are users of Trust digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

1.3. Online safety involves the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, email, gaming devices). Online safety is not just about technology, it is also about people and their actions.

1.4. The Trust has the highest regard for online safety in its schools in order to promote safe and responsible use of technology. We are committed to using new technology to enhance the curriculum and educational opportunities whilst equipping our pupils with the knowledge and understanding to stay safe and vigilant when online, both in school and outside.

1.5. Technology provides unprecedented access to new educational opportunities through online collaboration, learning and communication. At the same time, it can provide the potential for those in the Trust community to access material they should not access, or it may lead to them being treated by others inappropriately.

1.6. Online safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside and is integral to a school's ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Relationships, Sex and Health Education and include how staff and students should report incidents.

1.7. The Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

1.8. The Trust's 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.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Aims

2.1. The Trust aims to:

- Have robust processes in place to ensure the online safety of the Trust community.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers the Trust to protect and educate the whole Trust community in its use of technology, including mobile and smart technology (mobile devices).
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

3. Roles and Responsibilities

The Trust Board

3.1. The Trust Board has a strategic leadership responsibility for ensuring the Trust takes a whole Trust approach to online safety as outlined in this policy and that the Trust complies with duties under the related legislation and guidance listed later in this policy. The Trust Board has delegated some responsibilities, although retains accountability, as set out below

The Online Safety Link Trustee

3.2. The Trust Board has appointed an Online Safety Link Trustee who meet with the CEO and/or members of the Central Team each term. The Link Trustee will report back to the Trust Board normally by a written report.

3.3. All Trustees and Local Governors must:

- Ensure they have read and understand this Policy.
- Agree and adhere to the terms on acceptable use of the Trust's IT systems and the internet (refer to IT and Internet Acceptable Use Agreements).

The Chief Executive Officer (CEO)

3.4. The CEO is responsible through the Trust's Central Team and Headteachers for:

- Ensuring all staff undergo online safety training as part of child protection and safeguarding training, and that staff understand their expectations, roles and responsibilities around filtering and monitoring.
- Ensuring all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, so they are continually provided with the relevant skills and knowledge to effectively safeguard children.

- Holding 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).
- Ensuring the Trust has appropriate filtering and monitoring systems in place on Trust devices and school networks, and regularly review their effectiveness. Please refer to the Trust's Filtering and Monitoring Policy for details.
- Ensuring at least one member of the school's SLT is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Ensuring that online safety is a running and interrelated theme while devising and implementing the whole Trust approach to safeguarding and related policies and/or procedures.
- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring pupils are taught how to keep themselves and others safe, including keeping safe online.
- Ensuring that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). 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.
- Reviewing this policy annually and ensure the procedures and implementation are updated and reviewed regularly.

The Designated Safeguarding Leads (DSLs)

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the IT Department to make sure the appropriate systems and processes are in place for the school.
- Working with the Headteacher, IT Department and other staff, as necessary, to address any online safety issues or incidents.
- Managing all school online safety issues and incidents in line with the school's Safeguarding and Child Protection Policy.
- Ensuring that any school online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy.
- Ensuring that any school incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Behaviour policy.
- Updating and delivering staff training on online safety (appendix 1 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.
- 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.
- This list is not intended to be exhaustive.

IT Director

3.6. The Trust has a central approach to online safety. The IT Director 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.
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's IT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Reviewing online activity and concerns flagged through the filtering and monitoring systems to inform safeguarding practices and relevant risk assessments.
- This list is not intended to be exhaustive.

All Staff and Volunteers

3.7. 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 Trust's IT systems and the internet and ensuring that pupils follow the Trust's terms on acceptable use (refer to IT and Internet Acceptable Use Agreements).
- Knowing that each school's DSL is responsible for the school's filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by reporting this to the DSL or deputies immediately.
- Following the correct procedures by submitting a request to the Central Team if they need to bypass the filtering and monitoring systems for educational purposes.

- Working with the school's DSL to ensure that any online safety incidents are logged (see appendix 5) 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's 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'.
- Never using their Trust work device in any way that would violate the IT and Internet Acceptable Use Agreements. Work devices must be used solely for work activities.
- This list is not intended to be exhaustive.

Parents and Carers

3.8. Parents and carers are expected to:

- Notify a member of staff or the 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 IT systems and internet (refer to IT and Internet Acceptable Use Agreements).

3.9. 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 International
- Parent resource sheet – Childnet International

Visitors and all other Members of the Trust Community

3.10. Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (refer to IT and Internet Acceptable Use Agreements).

4. Educating Pupils About Online Safety

4.1. Pupils will be taught about online safety as part of the curriculum.
4.2. All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Primary Phase

4.3. In Key Stage (KS) 1, pupils will be taught to:

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

4.4. Pupils in Key Stage (KS) 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

4.5. By the end of the primary phase, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Secondary Phase

4.6. In KS3, pupils 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.

4.7. Pupils 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.

4.8. By the end of the secondary phase, pupils 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 which 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).

All Pupils

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

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

5. Raising Online Safety Awareness with Parents and Carers

5.1. The Trust will raise parents and carers’ awareness of internet safety in letters or other communications home, and in information on websites or school-specific online learning platforms.

5.2. This policy will also be shared with parents/carers.

5.3. If requested, the Trust and/or school will provide the following information to parents:

- What systems the Trust uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the Trust and/or school (if anyone) their child will be interacting with online.
- If parents and carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

Definition

6.1. 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's Behaviour Policy.)

Preventing and Addressing Cyber-bullying

6.2. To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

6.3. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying as part of planned sessions within the curriculum as well as additional sessions when responding to patterns or new triggers within local context.

6.4. 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.

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

6.6. The Trust and/or 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.

6.7. In relation to a specific incident of cyber-bullying, the each school will follow the processes set out in the school's Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

6.8. 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.

7. Examining Electronic Devices

7.1. The Headteacher, and any member of staff authorised to do so by the Headteacher (as set out in the school's Behaviour Policies), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or

- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

7.2. Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.
- Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

7.3. 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.

7.4. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

7.5. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

7.6. 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

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

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

7.8. Any complaints about searching for or deleting inappropriate images or files on pupils’ electronic devices will be dealt with through the Trust’s Complaints Policy and Procedure.

8. Artificial Intelligence (AI)

8.1. Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
8.2. The Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.
8.3. Schools will treat any use of AI to bully pupils in line with their Behaviour Policy.
8.4. 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.

9. Acceptable Use of the Internet Whilst on the Trust’s Sites

9.1. All pupils, parents and carers, staff, volunteers, local governors, and trustees are expected to sign an agreement regarding the acceptable use of the Trust’s IT systems and the internet (refer to IT and Internet Acceptable Use Agreements). Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.
9.2. 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.
9.3. The Trust will monitor the websites visited by pupils, staff, volunteers, local governors, trustees, members and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.
9.4. More information is set out in the IT and Internet Acceptable Use Agreements.

10. Pupils Using Mobile Devices in School

10.1. Any use of mobile devices in school by pupils must be in line with the IT and Internet Acceptable Use Agreements.
10.2. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the Trust and school’s Behaviour Policy, which may result in the confiscation of their device.

11. How the Trust will Respond to Issues of Misuse

11.1. Where a pupil misuses the Trust’s IT systems or internet, the Trust will follow the procedures set out in the Trust and school policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

11.2. Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and/or staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

11.3. The Trust will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

12.1. 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.

12.2. 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).

12.3. 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.

12.4. 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 .

12.5. Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.
- Each school's DSL and any 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.
- Trustees and local 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.

12.6. More information about safeguarding training is set out in each school's Safeguarding and Child Protection Policy.

13. Filtering and Monitoring Arrangements

13.1. Filtering and Monitoring systems are in place across all Trust devices and any device that logs onto the Trust's networks. Further information can be found in the Trust's Filtering and Monitoring Procedures (Appendix 3).

13.2. Each school's DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 2.

14. Links with Other Policies and Procedures

Safeguarding and Child Protection Policy
Behaviour Policy
Staff Disciplinary Procedures
Data Protection Policy and Privacy Notices
Complaints Policy and Procedure

Appendix 1: Online Safety Training Needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	

Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school’s acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school’s devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school’s ICT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 3: Filtering and Monitoring Procedures

Introduction: At 318 Education Trust, the safety and well-being of our children and young people is our utmost priority. We are committed to providing a safe and secure environment where CYP can learn, grow, and thrive. These procedures outline our approach to filtering and monitoring to ensure that students are protected from inappropriate content while using school-provided technology resources or whilst accessing the school network on personal devices.

1. Internet Filtering:

a. **Purpose:**

- Our school utilises advanced internet filtering technology to prevent access to inappropriate or harmful content. This ensures that students can explore online resources safely.

b. **Filtering Criteria:**

- The filtering system is configured to block access to websites and content that are deemed inappropriate for primary and secondary school-aged children. This includes, but is not limited to, explicit or violent material, gambling, pornography and social networking sites.

- **Geo-blocking is the practice of blocking network services based on the geographic region**. This practice is most commonly used when configuring firewall rules to prevent users from accessing web services from foreign countries, specifically those with higher than normal known bad actors. This may be a company requirement to comply with specific standards, or maybe you don't want your kids to access certain "free game sites" that download viruses and malware.

- **Cloudflare DNS**- We use this for all schools external DNS. Cloudflare provides tools to help safeguard the Internet experience for families and children at home. Users can get the same privacy-first DNS resolver with added filtering to protect schools from malware and adult content. 1.1.1.1. is also available for Families for home use.

- **Web blocker-** This uses a database that groups website addresses into content categories. When a user on your network tries to connect to a website, the Firebox looks up the address in the WebBlocker database and takes the action you specify for the content category. Category access is defined at Trust level. Websites are blocked by default until they are categorised by Watchguard. Websites are allowed and blocked by request by Trust IT services and, based on website risk and safeguarding concerns, are subject to the approval of SEND and Safeguarding Trust Consultant.

c. **Regular Review:**

- The filtering criteria are regularly reviewed and updated to adapt to evolving online threats and to provide the most comprehensive protection for our students. Schools will conduct a thorough online safety review annually and report these to the trust to identify new and emerging online risks.

2. Supervision and Monitoring:

Trust Responsibility:

- The Trust IT services will manage and maintain an agreed monitoring and alert system solution for all school owned devices that students use for online access. The current monitoring system is called *Content Keeper by Impero.* All devices owned by school will be monitored through this system. In addition, any devices brought from home that enter onto a school's wifi will be monitored through a login system. Devices using 4G will not be monitored and acceptable use will be determined at school level.   Alerts from the monitoring system will be live and will identify the precise device and username to enable DSLs to take swift action.

a. **DSL Responsibility:**

- Designated Safeguarding Leads (DSLs) at every school within the trust are responsible for understanding the filtering systems in place and for overseeing the monitoring alerts established by the Trust's software. They undergo training to effectively monitor these alerts and access pertinent information enabling them to respond appropriately should any concerns arise around inappropriate online activities or searches. DSLs will receive real-time alerts from our monitoring system and will be able to produce regular reports to identify patterns and trends to inform further safeguarding practices.

b. **Staff Responsibility:**

- All teaching staff are responsible for supervising and monitoring CYPs' online activities during school hours. They are trained to recognise and respond to any concerning behaviour or content. In line with our online safety policy, all staff receive regular update training about changes and new threats with regards to online safety.

c. **Acceptable Use:**

- CYPs are educated on responsible and safe internet use. They are made aware of the types of content they should avoid and are encouraged to report any uncomfortable situations to a trusted adult.

d. **Online Safety Education:**

- Our curriculum includes regular lessons on online safety, teaching students about online etiquette, privacy, and responsible use of technology.

3. Reporting and Response:

a. **Reporting Mechanism:**

- Any concerns regarding a student's online safety should be reported promptly to the designated safeguarding lead (DSL) or another trusted staff member.

b. **Response Protocol:**

- Upon receiving a report, the DSL will follow our established procedures for investigating and addressing the concern. This may involve contacting parents, involving appropriate authorities, or providing necessary support to the student.

4. Parental Involvement:

a. **Communication:**

- We believe in open and transparent communication with parents regarding our filtering and monitoring policies. Parents will be provided with information about the measures in place to protect their children online and can request this information from the school if required.

b. **Parental Controls at Home:**

- We encourage parents to implement appropriate filtering and monitoring measures at home to further support their child's online safety.