Author	Ross Weeks & Encarna Aparicio	Target group	All employees, consultants, and volunteers
Issued	September 2025		
Approved by	Executive Team	Next review	September 2027

Online Safety Policy

Aims

Anthem Schools Trust (the Trust) aims to:

- Have robust processes in place to ensure the online safety of students, staff and volunteers, including Anthem Community Council (ACC) members and Trustees, across all our Trust schools.
- 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalization, extremism, misinformation, disinformation and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

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

Roles and responsibilities

Headteacher

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

Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Safeguarding Policy.

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.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Working with the Headteacher, IT Team and other staff, as necessary, to address any online safety issues or incidents, including cyberbullying, in line with this policy, the Behaviour & Ethos Policy or the Anti-bullying Policy, ensuring these are logged and dealt with appropriately.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- 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.

The Anthem IT Team

The Anthem IT Team 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 on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring 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 for security vulnerabilities or malicious activity on a regular basis, including control environment tests.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any reported online safety incidents are logged and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

All staff and volunteers

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the Acceptable Use Agreement which sets out the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents.
- Working with the DSL to ensure that any online safety incidents are reported and dealt with appropriately in line with this policy, the Behaviour & Ethos Policy or the Anti-bullying 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.

Parents/Carers

Parents/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 Acceptable Use Agreement which sets out the terms of acceptable use of the Trust's ICT systems and internet.

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 and Childnet - Help and advice for parents and carers

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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating students about online safety

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

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 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
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online.

In **KS3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

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

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

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

Educating parents/carers about online safety

Each school will raise parents/carers' awareness of internet safety in communications home, and in information via their website or online learning platforms. This policy will also be shared with parents/carers.

Online safety may also be covered during parents' evenings.

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

Cyber-bullying

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. Further detail on bullying can be found in our Anti-Bullying Policy.

Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

The school may send information/leaflets on cyber-bullying to parents/carers 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 Anti-bullying and Behaviour & Ethos policies.

Acceptable Use Agreement

All students, parents/carers, staff, volunteers, including ACC members, are expected to sign the Trust Acceptable Use Agreement – an agreement regarding the acceptable use of the Trust's ICT systems and the internet. Visitors will be expected to read and agree to the 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 and visitors (where relevant) to ensure they comply with the above.

Use of mobile devices & examining phones and other electronic devices

Please refer to the school Behaviour & Ethos Policy and Mobile Phone Policy, available on the school's website, as well as the Staff Code of Conduct and Acceptable Use agreement.

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 three random words, in combination with numbers and special characters if required, or generated by a password manager
- not sharing the device among family or friends

Staff members must not use the device in any way that would violate the school's terms of acceptable use. Work devices must be used solely for work activities.

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

Internet Monitoring

Any devices that are connected to the school network will have their traffic monitored for appropriate use.

Where any device, including personal devices, are connected to the school's network, including Wi-Fi, their traffic will be subject to safeguarding searches. Any items flagged for concern will automatically be forwarded to the DSL for review.

How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, the school will follow the procedures set out in the Behaviour & Ethos 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 system or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Artificial intelligence (AI)

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

Anthem Schools Trust and its schools recognise 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.

Anthem Schools Trust and its schools will treat any use of AI to bully students very seriously, in line with our Behaviour & Ethos Policy and Anti-bullying Policy.

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

The DfE has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.

Training

All new staff members will receive training, as part of their induction, regarding 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.

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 students are at risk of online abuse

- Students can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

ACC members will receive training on online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every two years by the Trust.

Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- School Behaviour & Ethos Policy
- Anti-bullying Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices
- School's Concerns and Complaints Procedure
- Acceptable Use Agreement
- Staff Code of Conduct