The
TRIPLE CROWN
Centre

Online Safety Policy

Approved by Management Board Date of
Annual Review
Date of next review: September 2026

1. Aims

The Triple Crown Centre aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and members of the Management Board
- 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

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

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for 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 students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Management Board

The Management Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Management Board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Management Board will also make sure all staff receive regular online safety updates (e.g. via emails and staff meetings) as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to carry out their safeguarding duties effectively.

The Management Board will co-ordinate regular meetings with appropriate staff to discuss online safety and training requirements.

The Management Board will ensure students are taught how to keep themselves and others safe, including keeping safe online.

The Management Board will ensure The Triple Crown Centre has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The Management Board will ensure adherence to the DfE filtering and monitoring 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 requirements

The Management Board member who oversees online safety is our Safeguarding Link Governor. All

Management Board members will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms of acceptable use of the school's ICT systems and the internet
- Ensure online safety is a running and interrelated theme when devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that teaching about safeguarding, including online safety, is adapted for vulnerable students, victims of abuse and 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 students in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher and Designated Safeguarding Lead

The Headteacher is the Designated Safeguarding Lead (DSL) and is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the Headteacher as the school's Designated Safeguarding Lead (DSL) and Deputy Safeguarding Leads are set out in our Child Protection and Safeguarding policies, as well as relevant job descriptions.

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

- Ensuring staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Management Board 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
- Managing and addressing any online safety issues or incidents, in line with Triple Crown Centre'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 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

3.4 All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms of acceptable use of the school's ICT systems and the internet
- Ensuring that students follow the school's terms of 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 of those systems or processes failing
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring 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'

3.5 Parents/carers Parents/carers

are expected to:

- Ensure their child has read, understood and agreed to the terms of acceptable use of the school's ICT systems and internet
- Notify the Headteacher of any concerns or queries regarding this policy

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.6 Visitors and members of the community

Visitors and members of the community who use the Triple Crown Centre'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 of acceptable use.

4. Educating students about online safety

Students will be taught about online safety as part of the PSHE curriculum: 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
- To recognise inappropriate content, contact and conduct
- 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

The safe use of social media and the internet will also be taught:

- In other subjects where relevant
- Through school assemblies and Achievement Mentor delivered sessions
- As part of whole school focus days

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

By the end of Year 11, 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
- 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)

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in newsletters, communications home and in information via our website.

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

Concerns or queries about this policy can be raised with the Headteacher.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to themselves or others. Students will be encouraged to report any incidents and we will ensure students know how to do so. This includes reporting as a witness, as well as a 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, members of the Management Board and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The Triple Crown Centre also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Triple Crown Centre's 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.

If the Headteacher/DSL has reasonable grounds to suspect possessing that material is illegal, they will report the incident and provide the relevant material to the police as soon as is reasonably practicable. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device 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 member of staff is other than the Headteacher and they deem the search not to be urgent, they will seek advice from Headteacher
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members may examine and, in exceptional circumstances, erase any data or files on an electronic device they have confiscated, where they believe there is a 'good reason' to do so.

When deciding 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 and/or
- Disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, the Headteacher (or Deputy DSL in the Headteacher's absence) will 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, the Headteacher (or Deputy DSL in the Headteacher's absence) will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, the Headteacher (or Deputy DSL in the Headteacher's absence) 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, the Headteacher (or Deputy DSL in the Headteacher's absence) may delete it if:

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

If the Headteacher (or Deputy DSL in the Headteacher's absence) 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 decide what to do next, in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

6.4 Artificial intelligence (AI)

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

The Triple Crown Centre 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.

The Triple Crown Centre 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.

7. Acceptable use of the internet in school

All students, staff, volunteers and members of the Management Board are expected to sign an agreement regarding the acceptable use of the Triple Crown Centre's ICT systems and the internet.

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.

Websites visited by students, staff, volunteers and the Management Board are monitored to ensure they comply with the above and restrict access through filtering systems.

8. Students using mobile devices in school

Students may bring mobile devices to school, but are not permitted to use them during the school day, except at lunchtime to listen to music.

Any breach of the acceptable use agreement by a student during mobile phone use at lunchtime may trigger disciplinary action in line with the Triple Crown Centre's Behaviour Policy, alongside confiscation of their device.

9. Staff using work devices outside school

Work devices must be used solely for work activities.

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

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

- Keeping the device password-protected, Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Not sharing the device among family or friends
- Seeking advice from the Headteacher, if they have any concerns over the security of their device

10. 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 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 Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Triple Crown Centre will consider whether serious incidents, including those that involve illegal activity or content, should be reported to the police.

11. Training

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

All staff members will receive refresher training at least once each academic year as part of safeguarding training. They will also receive relevant updates as required (e.g. 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
- All children and young people are at risk of online abuse
- Physical abuse, sexual violence and initiation type violence can all contain an online element
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing abusive images and pornography to those who don't want to receive such content

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 weigh up the risks
- Develop the ability to influence students to make the healthiest choices and keep them safe from harm

The Headteacher/DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, in line with the DfE and Local Authority's expectations. They will also update their knowledge and skills in relation to online safety at regular intervals and at least annually.

Members of the Management Board will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding policies and The Triple Crown Centre's Safeguarding Training Logs.

12. Policy Monitoring arrangements

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the Management Board. Annual review is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies/documentation

This Online Safety Policy is linked to The Triple Crown Centre's:

- Child Protection Policy
- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Remote Leaning Policy
- Social Media Policy
- Data Protection Policy and Privacy Notice
- Student Acceptable Use Agreement
- Staff Disciplinary Policy
- Complaints Procedure