

St Benedict's Catholic High School

ANTI CYBERBULLYING POLICY (Addendum to Behaviour Policy) 2026-2027

Approved by ¹	
Name:	Kayleigh Daniels
Position:	Chair of Governors
Signed:	
Date:	September 2026
Review date ² :	September 2027



St Benedict's
Catholic High
School

1971

ANTI CYBERBULLYING POLICY

(Addendum to Behaviour Policy)

Rationale

Young people today use a wide range of digital technologies - social media, messaging apps, gaming platforms, livestreaming, online forums, and AI-powered tools - to connect, learn, and socialise. While most interactions are positive, some individuals misuse technology to harass, intimidate, or exploit others. This includes not only traditional forms of cyberbullying but also AI-enabled risks, such as manipulated images (deepfakes), impersonation, and AI-generated harmful content. Our school recognises these risks and is committed to providing a safe, respectful environment where all students use technology responsibly.

Definition

Cyberbullying is when someone is tormented, threatened, harassed, humiliated, or targeted using digital technologies. This includes but is not limited to:

- Social media platforms, messaging apps, livestreams, and online games
- Mobile phones, tablets, computers, and other connected devices
- AI-generated or manipulated content used to embarrass, threaten, or misrepresent others

Cyberbullying can take many forms, such as spreading rumours, sharing private information, excluding individuals from online groups, creating fake profiles, or using AI tools to impersonate or degrade others. Cyberbullying takes place between children; but also across different age groups.

Policy

St Benedict's Catholic High School is committed to developing a safe environment where the students act respectfully and positively towards each other in acceptable and non-threatening ways, we do this by:

- Promoting digital respect and responsibility
- Educating students and staff on safe, ethical use of technology and AI
- Responding quickly and appropriately to incidents
- Working in partnership with parents, carers, and external agencies.

Cyberbullying is bullying. It has the same consequences as other types of bullying. Each situation will be dealt with individually, in line with the school Behaviour and Online Safety Policy.

Procedure

Staff here have the responsibility to ensure that:

- all forms of cyberbullying and AI misuse are prohibited
- staff are aware of cyberbullying and are able to identify and look for signs of occurrence among the students
- students have been made aware of the consequences of cyberbullying and AI misuse in St Benedict's
- a code of conduct is in use for technology, including computers and mobile phones, whilst on the school premises
- all cases of cyberbullying are reported to the Online Safety Lead (OSL) and the Senior Assistant Headteacher (SAHT) and responded to promptly. These incidents are logged and appropriate action taken.
- there is supervision of technology that is effective for monitoring and deterring cyberbullying
- students are supported in cases of cyberbullying and AI Misuse.

Students must:

- Not engage in cyberbullying or AI misuse
- Not create, share, or promote AI-generated harmful content (e.g., fake images, videos, or messages)
- Not record or share unauthorised audio, video, or images of peers, staff, or community members
- Not breach privacy through unauthorised use of digital media
- Report incidents of cyberbullying or suspected AI misuse to a trusted adult or through the Safety Hub
- Support and stand up for peers who may be victims of bullying
- Use AI tools responsibly, ethically, and in line with school expectations

Strategies

St Benedict's promotes awareness and prevention of cyberbullying and AI misuse through:

- Posters, newsletters and assemblies
- Curriculum links in Computer Science, and Personal Development covering AI ethics, misinformation, and online behaviour
- Workshops and input from safeguarding professionals and the police
- The St Benedict's Safety Hub reporting app
- Guidance and promoted content via EduLink and Microsoft Teams
- Parent information sessions on online safety and AI awareness

Monitoring and Evaluation

Monitoring of progress towards implementation of this policy through termly meetings by the Online Safety Lead, Senior Assistant Headteacher (Behaviour and Standards) and the Designated Safeguarding Lead.

Supporting the person being bullied or targeted by AI content

1. Reassurance & Support
 - a. Acknowledge the victim's courage in reporting.
 - b. Inform parents/carers and provide pastoral support.
2. Practical Steps
 - a. Encourage victims not to retaliate.
 - b. Help them preserve evidence (screenshots, links, metadata).
 - c. Advise reviewing personal privacy and security settings.
 - d. Support them in blocking/reporting accounts or leaving harmful online spaces.
3. Containment & Action
 - a. If AI-generated content (e.g., fake images or deepfakes) has been shared, take steps to remove it.
 - b. Contact the platform host to request takedown of harmful or fake material.
 - c. Use disciplinary powers to confiscate devices where appropriate.
 - d. In cases of illegal activity (image-based abuse, threats, hate speech), inform the police.

There's plenty of online advice on how to react to cyberbullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips.

For Pupils: Cyberbullying and Safe Internet Use

Cyberbullying

Cyberbullying and AI misuse can occur across all platforms and devices. It's aim is to deliberately upset someone else.

Cyberbullying is bullying. It has the same consequences!

Cyberbullying takes place between children; but also across different age groups.

If you are being bullied, no matter how, let someone know.



Safe Internet Use (SMART+ Rules)

S Safe

Keep safe by being careful not to give out personal information - such as your name, email, phone number, home address or school name - to people you don't trust online.

M Meeting

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A Accepting

Accepting emails, IM messages or opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages!

R Reliable

Someone online may be lying about who they are, and information you find on the internet may not be reliable.

T Tell

Tell your parents, carers or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police.

+AI Artificial Intelligence

Use AI responsibly. Never create or share fake images, videos, or voices of others. Do not use AI tools to bully, impersonate, or spread false information. Always label AI-generated work when used for school projects. Be cautious - AI content can look real but may be misleading.

