



ANTI- CYBER BULLYING POLICY

Adopted	M. Davies September 2024
Committee	Members
Review Date	September 2025

Anti- Cyber Bullying Policy

Demetae Academy is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

1 Introduction

The use of technology has become a significant component of many safeguarding issues, including child sexual exploitation and radicalisation, where technology often provides the platform that facilitates harm.

An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

1. Content

Being exposed to illegal, inappropriate or harmful online content such as spam, pornography, fake news and disinformation, substance abuse, violence, misogyny, anti-Semitism, racism, radicalisation and extremism, and lifestyle sites that promote anorexia, self-harm or suicide.

2. Contact

Being subjected to harmful online interaction with other users. Examples include: peer-to-peer pressure, exposure to viruses and malware, anonymous online chat sites, cyber-bullying commercial advertising, personal data or identity theft, cyber-stalking and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

3. Conduct

Personal online behaviour that increases the likelihood of being harmed oneself or causing harm to others. Examples include threats to: health and well-being, such as gaming or social network addiction; online disclosure of personal information and ignorance of privacy settings; online bullying; 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 illegal conduct, including hacking, plagiarism, and copyright infringement of digital media, such as music and film.

4. Commerce

Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Cyber-bullying is defined as: “the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to cause harm or distress to another person”.

Demetae Academy has a duty to protect students and staff from such online activities and to ensure that they are aware of what constitutes cyber-bullying and the consequences of cyber-bullying, including its possible legal consequences. This policy takes account of guidance given by the KCSIE (September 2024).

The policy makes clear that failure to follow this protocol will constitute misconduct and will be dealt with under the school’s disciplinary procedures.

2. Aims

- To protect students and staff from harmful online activities
- Ensure all staff, students, parents and guardians understand what constitutes unsafe online behaviours and cyber-bullying
- Set clear expectations in terms of online behaviours and a clear framework of sanctions that will be imposed on those who do not meet them
- Need for staff, students, parents and guardians to work together to create a culture within which cyber-bullying is not tolerated
- Have well-understood mechanisms in place for instances of cyber-bullying to be reported and managed

- Ensure students know how to respond if they are a victim of cyber-bullying or are aware that it is taking place

3. What forms can cyber-bullying take?

Cyber-bullying can take many forms, notably including:

- threats and intimidation
- harassment or stalking
- vilification and defamation
- ostracizing, peer rejection and exclusion
- identity theft, unauthorized access and impersonation
- publicly posting, sending or forwarding personal or private information or images.

It is important to recognise that though cyber-bullying is a type of bullying, it differs from traditional bullying in certain ways.

These include the following:

- intrusion into personal space: victims will be equally subject to cyber-bullying inside as well as outside traditional safe spaces such as the home because they will receive the offensive material on their phones or personal computers.
- a greater audience: offensive messages or other content may be sent by and viewed by a large number of people.
- anonymity: cyber-bullies can post anonymously.
- longevity: offensive messages or other content can be copied, stored and resent potentially indefinitely.
- bystanders: bystanders can easily become perpetrators or accessories, for instance by not reporting, and even disseminating, upsetting messages or other content.
- multiple attacks: cyber-bullying can lead to a single incident being experienced as multiple attacks.

There are many ways in which offensive messages or other content can be created and disseminated. These include:

- email
- instant or direct messaging (e.g., via Snapchat, WhatsApp)
- social media sites (e.g., Facebook, Instagram, TikTok)
- chatrooms and message boards
- virtual learning environments.
- gaming sites and virtual worlds.
- video contact (e.g., through FaceTime, Zoom, MS Teams, Omegle, etc)

5. Staff roles and responsibilities

The Designated Safeguarding Lead (Dee Robins) has overall responsibility for organising and implementing the school's procedures for managing how staff and students are made aware of cyber-bullying and how the school handles incidents of cyber-bullying.

The DSL will:

- ensure that all incidents of cyber-bullying both inside and outside school are dealt with as soon as possible and will be handled according to the procedures set out in this policy.