

Cyberbullying and Online Safety Policy

Introduction

The College is committed to eliminating any form of electronic social aggression (Cyberbullying) and ensuring the online safety of all students. This policy outlines the measures taken to protect students from cyberbullying and other online risks, in accordance with the latest guidance.

What is Cyberbullying?

Cyberbullying is a threatening intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot defend themselves properly.

There are several forms of cyberbullying, including:

- Text message bullying: Sending unwelcome texts that are threatening or may cause unnecessary discomfort
- Phone call bullying: Making silent calls or leaving abusive messages. Using someone else's phone to harass others or disguise their numbers
- Email bullying: Sending bullying or threatening messages using someone else's number or a pseudonym for anonymity
- Picture/video clip bullying: Using phone cameras to make an individual feel threatened or embarrassed. 'Happy Slapping' involves filming and sharing physical attacks
- Chat room bullying: Sending menacing or upsetting responses to people in a web-based chat room
- Instant messaging bullying: Sending unpleasant messages during real-time conversations online
- Defamatory blogs: Posting defamatory content on websites
- Social media bullying: Bullying via platforms such as Facebook, Instagram, Snapchat, and Twitter

Preventative Measures

Students are expected to comply with the following when using College facilities. Misuse of College and/or workplace facilities may result in disciplinary action:

- Ensure that any communication through the internet and email is professional and related to learning
- Avoid contravening any internet or social media policy
- Keep passwords confidential and change them when prompted or when known by another user
- Use passwords that are not obvious or easily guessed
- Log off at the end of each session to ensure that no one else can use their e-learning account

- Promptly report if you suspect you have received a computer virus or spam (i.e., unsolicited email) or if you receive a message that is inappropriate or makes you feel uncomfortable
- Keep personal information including names, addresses, photographs, credit cards, and telephone numbers of yourself and/or others private
- Avoid using the electronic identity of another person to send messages to others or for any other purposes
- If contacted by the press or any other external organization about posts on their social networking site that relates to The College, notify your personal tutor, who will then report it to their Manager
- Do not take photos or videos of other members of the college community or work placement without their prior consent

Staff Responsibilities

All staff are required to be trained in identifying and responding to online risks. Staff responsibilities include:

- Mandatory staff training on online safety
- Record-keeping and reporting concerns
- Coordinating responses to cyberbullying incidents
- Liaising with external agencies

Filtering and Monitoring

The College uses appropriate filtering and monitoring systems to detect and prevent harmful online activity. These systems are continually reviewed and updated to ensure the safety of all students.

Education and Curriculum

Cyberbullying and online safety are embedded in the curriculum. Students are educated on the risks of communication technologies and the consequences of their misuse.

Reporting Mechanisms

The College provides clear, accessible reporting routes for students, including anonymous options. A flowchart or visual guide for handling incidents is available to ensure students know how to report concerns.

Safeguarding Culture

The College promotes a whole-college approach to safeguarding, including regular policy reviews, student voice and participation, and collaboration with parents and carers.

Procedure in the Event of Cyberbullying

Any threat of violence, instance of cyberbullying, or electronic harassment must be reported to a senior manager at the College. The following steps will be taken:

- A prompt investigation will be initiated by the Principal or Vice Principal Quality
- Disciplinary procedures will apply if there is evidence of misconduct
- Website hosts/Social media platforms will be asked to amend or remove material where appropriate
- Report to the police as necessary
- Offer support and stress counselling if necessary
- Inform parents/guardians where appropriate
- Fitness to Study or Fitness to Practise concerns involving cyberbullying will require disclosure to the Professional Body

Further Information

For more information, visit: http://www.antibullying.net

Policy Reviewed: May 2025 Next Review Due: May 2026