Cyber-bullying Policy

2025-2026

Reviewed by Dee Robins: 7 June 2025

Approval by the Board: 3 September 2025

Next review: June 2026

1 Introduction

The use of technology has become a significant component of many safeguarding issues, including child sexual exploitation, radicalisation and sexual predation, where technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole college 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 students 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”. MPW has a duty to protect students and staff from such online activities and to ensure that they 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 DfE’s Cyber bullying: advice for headteachers and school staff and Advice for parents and carers on cyber bullying along with the guidance given in KCSIE (September 2024). In addition, MPW is regularly advised by the local authority on matters relating to safer on-line behaviours. The college’s e-safety policy sets out the permissions and restrictions which apply to all students’ use of the internet, including social media, email and other messaging applications. The policy makes clear that failure to follow this protocol will constitute misconduct and will be dealt with under the college’s disciplinary procedures.

This policy should be read in conjunction with the e-safety policy, anti-bullying policy, safeguarding policy, PSHE policy, the policy for promoting good behaviour and the staff code of conduct.

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 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/videos.
    - NB: AI is increasingly being used to create nude and semi-nude images and videos.

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)
- chatrooms and message boards
- virtual learning environments.
- gaming sites and virtual worlds.
- video contact (e.g., through FaceTime, Zoom, MS Teams, Omegle, etc)

4 Staff roles and responsibilities

The Designated Safeguarding Lead (Seán Buckley) has overall responsibility for organising and implementing the college's procedures for managing how staff and students are made aware of cyber-bullying and how the college 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.
- ensure that all policies relating to safeguarding, including cyber-bullying, are reviewed and updated regularly.
- ensure that all staff know that they need to report cyber-bullying issues to the E-safety Co-ordinator (Susannah Gordon) or the Designated Safeguarding Lead.
- ensure that parents/guardians know about the cyber-bullying policy and how to access it from the college's VLE.
- ensure that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology inside and outside of college as set out in the e-safety policy and the Staff Code of Conduct.

The E-Safety Co-ordinator (Susannah Gordon, DDSL) will:

- ensure that all students are given clear guidance on the use of technology safely and positively both in school and beyond including how to manage their personal data and how to report abuse and bullying online.
- provide annual training for parents/carers on online safety and the positive use of technology
- ensure the school's Acceptable Use Policy, Guidelines for Staff when Children are using Digital Devices, and Children's Use of Digital Devices are reviewed annually
- provide annual training for staff on the above policies and procedures
- provide annual training for staff on online safety
- plan and deliver a curriculum on online safety in computing lessons which builds resilience in students to protect themselves and others online.
- plan a curriculum and support PSHE staff in delivering a curriculum on online safety which builds resilience in students to protect themselves and others online.

The IT Group Manager (Carlos Noguiera) will:

- ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Designated Safeguarding Lead to safeguarding issues. MPW uses NetSupport DNA for this purpose.

All staff will:

- Read the e-safety policy, cyber-bullying policy, safeguarding policy and staff code of conduct at the start of term and thereby be aware of what constitutes cyber-bullying and the measures the college has for preventing cyber-bullying.
- Receive regular updates and CPD of online safeguarding and cyber-bullying through Handsam, staff inset days and e-bulletins to ensure they are fully informed of any changes, updates or alterations.

  Note: Appendix A provide a list of further resources staff may consult.

5 Staff procedures for reporting an incident of cyber-bullying

If you suspect or are told about a cyber-bullying incident, you should follow the following procedure.

- Record the information on the screen: the time, date, content and sender.
    - If the content is in the form of a spoken message, make a transcript of it.
    - If possible (e.g., where a computer is involved), print out the content or save a screenshot.
- Request that the member of staff or student save the information.
- Inform the Designated Safeguarding Lead via MyConcern as soon as possible.

6 Guidance for students

If you believe you or someone else is the victim of cyber-bullying, you must speak to a member of staff as soon as possible.

All students should heed the following advice:

- Report your concerns to a member of staff immediately
- Reports can also be made anonymously via the Whisper reporting tool
- Never answer abusive messages or emails.
- Never reply to messages from people you do not know
- Always save abusive messages. Do not delete any messages until you have been told that it is acceptable to do so by one of the safeguarding team
- Never give out personal details or contact information online
- Think carefully before befriending anyone online
- On social media sites, set your privacy settings appropriately
- Protect your passwords. Do not share them with anyone and change them regularly
- Always lock the computer you are working at and, if a college computer, log off when you have finished.

7 Guidance for parents/guardians

It is vital that parents and guardians work alongside staff and students to ensure that all students are aware of the existence of cyber-bullying and the consequences of becoming involved in it. They should:

- Be aware of their son or daughter's online life, especially when they are at home.
- Follow the above guidance for staff should they have concerns. Parents/guardians may inform the safeguarding team directly or via their son or daughter's Director of Studies.
- Be aware that incidents of cyber-bullying can occur during college holidays and that therefore the college will treat them just as it would have had they happened during term time.
- Make use of the college's resources for informing them of issues relating to cyber-bullying. The college runs parent talks and provides access to relevant resources on cyber-bullying via the parent portal. The college's safeguarding team also send out e-bulletins that provide access to further resources and guidance on home monitoring and guidance.
- Be aware of the consequences should their son or daughter be a perpetrator of cyber-bullying.

8 Sanctions

While the normal sanctions for bullying still apply, additional or alternative sanctions connected to information and communications technology may be imposed. For instance, students involved in cyber-bullying may have limitations placed upon their ICT, internet and mobile phone usage at college. Students who have cyber-bullied may be asked to undergo specific anti-cyber-bullying training, to ensure they understand the impact of their actions.

MPW reserves the right to confiscate devices where there is clear evidence of misuse, and to exclude students in the most serious cases. The college reserves the right to charge a student or their parents/guardians for any costs incurred to the college, or to indemnify any significant liability incurred by the college, as a result of a breach of this policy.

9 Criminal law

Cyberbullying in itself is not a crime and is not covered by a specific law in the UK. However, by committing an act of cyberbullying, a person may be committing a criminal offence under a number of different acts. This includes the following: Protection from Harassment Act (1997), Malicious Communications Act (1988), Communications Act (2003), Public Order Act (1986) and the Computer Misuse Act (1990). For example, under the Malicious Communications Act, any person who sends a communication (written or electronic) which conveys a message which is indecent or grossly offensive, a threat, of information which is false or known or believed to be false by the sender is a criminal offence if the purpose of sending it is to cause distress or anxiety to the recipient. Those convicted of criminal offences under any of these Acts are liable to face a prison sentence, a substantial fine or even both.

10 Record keeping

As with other types of bullying, records of all investigations, including student and parental meetings, telephone conversations, e-mails and other communications must be kept and placed in the relevant student files. If there are issues of child protection and safeguarding, a separate record will be kept confidentially by the Designated Safeguarding Lead and the college's safeguarding and child protection procedures will be followed.

11 Monitoring and Review

The policy is reviewed annually in June in conjunction with a review of the anti-bullying policy. The review is conducted by the college's Designated Safeguarding Lead, Seán Buckley, and the Deputy Designated Safeguarding Leads (DDSLs), Naeem Gofur, Susannah Gordon, Nikki Morris, Egle Plioplyte and Rachel Sherman along with the SENDCO Amy Sivadasan. who monitor the implementation and effectiveness of this policy. The review includes an analysis of the procedures used to raise awareness of cyber-bullying, to prevent and to deal with cyber-bullying, as well as mapping cyber-bullying incidents, their provenance and prevalence.

12 Other Relevant Documentation

- Anti-bullying Policy
- Child Protection and Safeguarding Policy
- PSHE policy and Scheme of Work
- Behaviour Policy
- Acceptable Use Policy
- E-safety Policy
- Staff Code of Conduct

Appendix A: Resources for schools and colleges

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on sexting-in-schools-and- colleges and using-external-visitors-to-support-online-safety-education

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Lucy Faithfull Foundation's StopItNow resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Teaching resources for staff

- Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing.
- PSHE association provides guidance to schools on developing their PSHE curriculum
- Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources
- UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education includingplanning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning