

Cyberbullying Policy

2026-2027

Reviewed by Jon Slay: 4 September 2026

Approval by the Board: 15 September 2026

Next review: June 2027

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.

Cyberbullying may constitute a safeguarding concern and a form of child-on-child abuse. It may occur inside or outside college, and online abuse may occur independently or alongside face-to-face abuse. Where cyberbullying raises a safeguarding concern, the college's Safeguarding Policy and child-on-child abuse procedures will take precedence over disciplinary procedures.

Online harm may include the creation, manipulation or sharing of images, audio or video using artificial intelligence, including deepfakes; the creation or circulation of AI-generated child sexual abuse material; the non-consensual creation or sharing of intimate imagery; and financially motivated sexual extortion (FMSE). Such incidents will be treated as safeguarding concerns and managed in accordance with the college's Safeguarding Policy and KCSIE.

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, antisemitism, 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 or generative AI applications that simulate human interaction, including 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.
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 including AI generated explicit images 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. Concerns about phishing or financial scams affecting students or staff should be reported in accordance with the college's safeguarding and IT reporting procedures.

This policy focuses specifically on cyberbullying within this wider online safety framework, including how the college prevents, identifies, reports, records and responds to incidents affecting students or staff.

Cyberbullying 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 are aware of what constitutes cyberbullying and the consequences of cyberbullying, 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 section 6. In addition, MPW is regularly advised by the local authority on matters relating to safer online 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.

2 Aims

- Protect students and staff from harmful online activities
- Ensure all staff, students, parents and guardians understand what constitutes unsafe online behaviours and cyberbullying
- 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
- Promote the need for staff, students, parents and guardians to work together to create a culture within which cyberbullying is not tolerated
- Maintain well-understood mechanisms in place for instances of cyberbullying to be reported and managed
- Ensure students know how to respond if they are a victim of cyberbullying or are aware that it is taking place

3 What forms can cyberbullying take?

Cyberbullying can take many forms, notably including:

- threats and intimidation
- sexual harassment, including consensual and non-consensual sharing of nudes/semi-nudes; unwanted explicit content; sexualised online bullying; unwanted sexual comments/messages; sexual exploitation, coercion and threats; and coercing someone into sharing images or performing sexual acts online
- abusive, discriminatory, misogynistic or misandrist messages, including prejudice-based or discriminatory cyberbullying
- harassment or stalking
- vilification and defamation
- ostracising, peer rejection and exclusion
- identity theft, unauthorised access and impersonation
- publicly posting, sending or forwarding personal or private information, images or videos
- sending or sharing pornography or other explicit material with someone who does not wish to receive it

NB: Cyberbullying may involve the use of artificial intelligence, including generative AI, to create, alter or distribute false, abusive, humiliating or sexualised material about another person. This includes AI-generated or digitally altered nude or semi-nude images ('deepfakes' or 'deep nudes'), impersonation, fabricated messages, voice cloning and other manipulated content.

It is important to recognise that though cyberbullying 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 cyberbullying 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: cyberbullies can post anonymously.
- longevity: offensive messages or other content can be copied, stored and resent potentially indefinitely.
- multiple attacks: cyberbullying 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-calling, livestreaming and online meeting platforms

4 Staff roles and responsibilities

The Board retains strategic oversight of online safety, including cyberbullying and filtering and monitoring arrangements. It receives relevant safeguarding information through established reporting arrangements and seeks assurance that the college's systems, training and procedures remain effective.

The Designated Safeguarding Lead (Jon Slay) has overall responsibility for organising and implementing the college's procedures for managing how staff and students are made aware of cyberbullying and how the college handles incidents of cyberbullying.

The DSL will:

- ensure that all incidents of cyberbullying, both inside and outside college, are dealt with as soon as possible and handled according to the procedures set out in this policy.
- ensure that all policies relating to safeguarding, including cyberbullying, are reviewed and updated regularly.
- ensure that all staff know that they need to report cyberbullying issues to the Online Safety Co-ordinator (Simon Baldwin: simon.baldwin@mpw.ac.uk) or the Designated Safeguarding Lead (Jon Slay: jon.slay@mpw.ac.uk).
- ensure that parents/guardians know about the cyberbullying policy and how to access it.
- ensure that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology inside and outside college, as set out in the E-safety Policy and the Staff Code of Conduct.
- Where cyberbullying involves children under 18, the DSL/DDSL will consider whether the behaviour constitutes child-on-child abuse and will assess the safeguarding needs of both the child who has experienced the behaviour and the child alleged to have caused harm. The college recognises that a child displaying harmful behaviour may themselves have unmet safeguarding or welfare needs.

The Online Safety Co-ordinator (Simon Baldwin) will:

- ensure that all students are given clear guidance on the use of technology safely and positively both in college and beyond including how to manage their personal data and how to report abuse and bullying online.
- provide annual training for parents/guardians on online safety and the positive use of technology
- ensure the college's Acceptable Use Policy and Guidelines for Staff 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 students' resilience to protect themselves and others online.
- ensure staff and students receive appropriate guidance on the safe and responsible use of generative AI, including safeguarding risks arising from AI-generated content, simulated interactions, deepfakes, data protection, intellectual property and inappropriate or harmful outputs.

The IT Group Manager (Carlos Nogueira) will:

- manage the use of Classroom Cloud for filtering and monitoring the use of college devices, including personal devices connected to MPW Wi-Fi.
 - The effectiveness of Classroom Cloud will be reviewed at least once every academic year by the SLT member responsible for filtering and monitoring, supported by the DSL and IT support/provider. The review will include checks that filtering operates appropriately on all internet-connected devices in all relevant college locations, and a record of these checks will be retained.

All staff will:

- challenge inappropriate online behaviour and not dismiss abusive, discriminatory or sexually harmful online behaviour as “banter”, “having a laugh” or part of growing up.
- read the E-safety Policy, Cyberbullying Policy, Safeguarding Policy and Staff Code of Conduct at the start of the academic year and thereby be aware of what constitutes cyberbullying and the measures the college has for preventing cyberbullying.
- Receive regular updates and CPD on online safeguarding and cyberbullying, staff inset days and e-bulletins to ensure they are fully informed of any changes, updates or alterations.

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

5 Staff procedures for reporting an incident of cyberbullying

If you suspect or are told about a cyberbullying incident, you should follow this 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.
- On receipt of a report, the DSL/DDSL will assess the nature and seriousness of the concern, including safeguarding risk, whether the bullying threshold has been met, whether the behaviour involves child-on-child abuse, sexual harassment, intimate imagery, discrimination, coercion, exploitation, threats, criminal behaviour or wider online safety concerns, and whether external agencies, including the police or children's social care, should be involved. The college will also consider the welfare and safeguarding needs of all students involved, including any student alleged to have caused harm. Incidents may be managed under the Anti-bullying Policy, Behaviour Policy or Safeguarding Policy, and will be supported by proportionate pastoral, safeguarding and disciplinary responses as appropriate.
- Where a report is made through the online reporting tool, the safeguarding team will monitor and triage the concern. Anonymous reports will still be reviewed, recorded and acted upon as far as the available information allows. Students may also report concerns directly to the DSL or a DDSL.
- Where the concern involves a nude or semi-nude image, sexually explicit image or suspected illegal image of a person under 18, staff must not intentionally view, copy, print, screenshot, download, forward or otherwise share the image. The DSL/DDSL must be informed immediately and the college's procedures for responding

to nudes and semi-nudes must be followed. Where appropriate, a device may need to be secured to preserve evidence and passed to the police.

6 Guidance for students

If you believe you or someone else is the victim of cyberbullying, you must speak to a member of staff as soon as possible. Students who report cyberbullying or other online abuse will be taken seriously, supported and kept safe. They will not be made to feel that they are creating a problem by making a report or be made to feel ashamed.

All students should heed the following advice:

- report your concerns to a member of staff immediately
- reports can also be made anonymously via the online reporting tool
- Never answer abusive messages or emails
- Never reply to messages from people you do not know
- Never share, forward or screenshot nude, semi-nude, sexual, humiliating or abusive images of another person.
- 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 cyberbullying and the consequences of becoming involved in it. They should:

- be aware of their child'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 child's Personal Tutor.
- Be aware that incidents of cyberbullying 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 cyberbullying. The college runs parent talks and provides access to relevant resources on cyberbullying 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 online safety.
- be aware of the consequences should their child be involved in cyberbullying.

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 cyberbullying may have limitations placed upon their ICT and internet usage at college. Students who have cyberbullied may be asked to undergo specific anti-cyberbullying training, to ensure they understand the impact of their actions.

MPW staff may confiscate or secure a device where there is clear evidence of misuse, where this is necessary to safeguard students, preserve evidence or prevent further harm. Any such action will be lawful, proportionate and

in accordance with the college's policies on promoting good behaviour, safeguarding, and searching, screening and confiscation.

Students' use of personal mobile phones and other connected devices whilst on college premises is governed by the college's Behaviour, Acceptable Use and E-safety policies. Misuse of a personal device to bully, harass, intimidate or abuse another person may result in restrictions on its use and/or disciplinary action.

Any sanction will be proportionate, take account of the circumstances of the incident and the needs of the students involved, and be applied alongside appropriate safeguarding or pastoral support.

9 Criminal law

Cyberbullying is not a single specific criminal offence in the UK. However, particular behaviours associated with cyberbullying may amount to criminal offences under communications, harassment, intimate-image, sexual offences, public order, computer misuse or other legislation. This may include sending grossly offensive, threatening, indecent or knowingly false communications; harassment or stalking; sharing or threatening to share intimate images; creating or sharing sexual images of children; unauthorised access to accounts or devices; impersonation; or conduct motivated by hostility towards a protected characteristic. Where the college believes that a criminal offence may have been committed, the DSL will consider whether referral to the police and/or children's social care is required, in line with the college's Safeguarding Policy.

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 on MyConcern in accordance with the college's Safeguarding Policy.

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, Jon Slay, and the Principal and DDSL, Ann Meisner and the SENCO, Elpida Christianaki, who monitor the implementation and effectiveness of this policy. The review includes an analysis of the procedures used to raise awareness of, prevent and respond to cyberbullying, as well as mapping cyberbullying incidents, their provenance and prevalence. This will include consideration of the number and type of incidents, repeat patterns, discriminatory or protected-characteristic elements, platforms or locations involved, response times, student and parent feedback, and any curriculum, pastoral, staff training or technical actions arising from incidents.

12 Other Relevant Documentation

- Anti-bullying Policy
- 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

The following resources provide authoritative support for staff, students and parents/guardians. The list is not exhaustive and is reviewed annually alongside this policy to ensure that links and guidance remain current.

Reporting online abuse and harmful content

- [CEOP Safety Centre](#) – for reporting concerns about online sexual abuse, exploitation or inappropriate sexual contact involving a child.
- [Report Remove](#) – Childline and IWF support for young people to report and seek removal of sexual images or videos of themselves.
- [Report Harmful Content](#) – for advice and support in reporting harmful online content to platforms.
- [Internet Watch Foundation](#) – for reporting child sexual abuse imagery online and accessing support resources.

Online safety and cyberbullying

- [UK Safer Internet Centre](#) – online safety advice, helplines, reporting routes and resources for schools, parents and young people.
- [Childnet](#) – practical guidance for schools, students and parents on cyberbullying, digital wellbeing and online safety.
- [Internet Matters](#) – age-specific guidance for parents and carers, including privacy settings, parental controls and online wellbeing.
- [Anti-Bullying Alliance](#) – guidance and resources on preventing and responding to bullying, including cyberbullying.
- [SWGfL](#) – online safety policy, training and practice resources for education settings.

Sexual abuse, exploitation and emerging online harms

- [CEOP Education](#) – education resources on online sexual abuse, exploitation, image sharing and digital safety.
- [National Crime Agency](#) – guidance on online child sexual exploitation, financially motivated sexual extortion and related threats.
- [Internet Watch Foundation](#) – resources on child sexual abuse imagery, including reporting and removal pathways.
- [Lucy Faithfull Foundation / Stop It Now](#) – advice for adults concerned about harmful sexual behaviour or online sexual risks.

Advice for governing bodies/proprietors and senior leaders

- [Searching, screening and confiscation](#) – advice from the Department for Education for schools on searching pupils and confiscating items, including mobile phones.
- [NSPCC online safety for schools](#) – guidance on online safety arrangements and safeguarding practice.
- [London Grid for Learning](#) – online safety, filtering, monitoring and safeguarding resources for schools and colleges.
- [Safer Recruitment Consortium](#) – guidance for safe working practice, relevant to staff conduct and professional boundaries.
- [Educate Against Hate](#) – practical advice on protecting children from extremism and radicalisation.

Support for children

- [Childline](#) – free and confidential advice and support for children and young people.

- [Report Harmful Content](#) – support with reporting harmful online content.
- [CEOP Safety Centre](#) – advice and reporting route for online abuse or exploitation.

Parental support

- [Childnet parent and carer toolkit](#) – guidance to help parents discuss online life, set boundaries and find support.
- [Internet Matters](#) – age-specific online safety checklists, parental controls guidance and practical advice.
- [Parent Zone](#) – support for families on online safety, digital wellbeing and online risks.
- [Parent Info](#) – guidance for parents from Parent Zone and the National Crime Agency.
- [Let's Talk About It](#) – advice for parents and carers on online radicalisation risks.