Cyber bullying (KCSIE 2026) Summary

Your Core Responsibilities

All staff (including volunteers, contractors and agency staff) must:

- **Model safe online behaviour** at all times.
- **Supervise pupil device use directly** — screens must be actively monitored.
- **Report ALL online safety concerns immediately** to the DSL/DDSL or Head.
- **Log concerns on CPOMS** using the correct category (contextual / non-contextual).
- **Follow the Acceptable Use Policy (AUP)** and ensure pupils do the same.
- **Use only school systems** (email/Teams) for communication with pupils/parents.
- **Never investigate harmful content yourself** — do not view, save, delete or forward.
- Maintain the mindset: **"It could happen here."**

Linked policies: Child Protection & Safeguarding; Online Safety; Behaviour; Child-on-Child Abuse; Nudes & Semi-Nudes; AI & Online Risks; Filtering & Monitoring; Prevent.

Key Online Risks (KCSIE 2026)

Staff must understand the four categories of online risk:

- Content – harmful/illegal content (pornography including AI-generated, extremism, self-harm, hate, misinformation).
- Contact – grooming, coercion, blackmail, unsafe contact via apps/games/livestreaming.
- Conduct – cyberbullying, sharing nudes/semi-nudes, harmful challenges, hacking, patterning.
- Commerce – scams, phishing, gambling, subscription traps.

Patterning – Staff Summary

- Patterning = filming child-on-child assaults and sharing the footage online to humiliate or shame.
- Trolling – inflammatory messages and videos designed to create conflict, hostility and bait others and intend to create harm. A form of cyber aggression
- It is child-on-child abuse and a safeguarding incident.
- Never view the footage — even if pupils try to show it.
- Confiscate the device, reassure the pupil, report immediately to the DSL.
- Do not ask pupils to delete footage — this may destroy evidence.
- DSLs will assess police threshold, online harm, filtering alerts and wellbeing impact.
- Staff must log all concerns on CPOMS and use **Whistleblowing** if concerns are not addressed.

Misogyny

This is a form of online harm. Misogynistic content — including sexist messages, gender-based harassment, sexualised comments, or hostility towards girls/women — is treated as online abuse and a safeguarding concern.

Filtering & Monitoring – What You Must Do

BA MAT uses WatchGuard, FastVue, TalkTalk Education Broadband and Primary Technologies.
Staff must:

- Know that all devices and networks are monitored.
- Close all apps before arriving on site (personal devices trigger alerts).
- Connect personal devices to school Wi-Fi when on site.
- Report any filtering/monitoring failures to the DSL or Head.
- Request filtering bypass only via the Head (for planned curriculum needs).
- Ensure filtering does not unreasonably restrict teaching and learning.

Linked policy: Filtering & Monitoring Policy.

AI, Deepfakes & Emerging Risks

Staff must:

- Treat **AI-generated sexual images of children as illegal CSAM**.

- Report any AI-generated bullying, nudification, impersonation or deepfake content.
- Never ask to see or delete imagery — follow Nudes & Semi-Nudes guidance.
- Use only Trust-approved AI tools.

Linked policies: AI & Online Risks; Deepfakes; HSB; Nudes & Semi-Nudes.

Cyberbullying & Online Abuse

Cyberbullying includes:

- abusive messages
- sharing pornography or harmful images
- impersonation
- sexual harassment online
- AI-generated bullying
- patterning

All incidents are safeguarding concerns and must be logged on CPOMS.

Linked policies: Cyberbullying; Behaviour; Child-on-Child Abuse.

Teaching & Classroom Practice

In every lesson involving devices:

- Reinforce safe search and safe use expectations.
- Guide pupils to checked, appropriate sites.
- Record which device each pupil/group is using.
- Address online issues raised in class and log concerns.
- Teach pupils to evaluate online content (fake news, hoaxes, deepfakes).
- Teach pupils how to report concerns (trusted adults, CEOP, Childline, Report Remove).
- Use Purple Mash (Computing), Kapow (PSHE/RSE), and Education for a Connected World.

Staff Devices & Data Protection

Staff must:

- Use strong passwords (three random words).
- Ensure encryption and auto-locking.
- Keep devices updated.
- Never store personal data locally.
- Delete emails containing personal data when no longer needed.
- Seek IT support if concerned about device security.

Linked policy: Data Protection Policy and safely using digital devices and social media policy

Mobile Devices (Staff & Pupils)

- Year 6 pupils may bring phones for travel only — phones must be handed in on arrival.
- Staff must follow BYOD expectations and connect to school Wi-Fi.
- Personal device misuse may lead to disciplinary action.

Linked policies: Safely Using Digital Devices & Social Media; Cyber Policy (BYOD).

When to Report Externally

DSLs/Heads may contact:

- **Police / CEOP / IWF / ICS / Prevent** for illegal content, significant harm, extremism, or exploitation.

Staff must **not** contact external agencies directly — report internally first.

Quick Reporting Routes

- **DSL / DDSL** – all online safety concerns
- **Head** – filtering bypass, offensive emails, device misuse
- **IT Technician** – device security concerns
- **CPOMS** – record all incidents

Bourne Alliance
Multi Academy Trust

Policy document for: Cyber bullying (online bullying)

Due for review: Spring 2027

Reviewed Sept 2026 with changes to KCSIE 2026

This policy forms part of the Trust Safeguarding and Child Protection policy and online safety policy and gives specific school actions in relation to their context. This policy aligns with **KCSIE 2026**, the **Online Safety Act 2024**, and the **DfE Filtering & Monitoring Standard**.

This policy must be read alongside:

- Safeguarding & Child Protection Policy
- Behaviour Policies for each school
- Child-on-Child Abuse Policy
- Online Safety Policy
- Filtering & Monitoring Policy
- AI & Online Risks Policy
- Deepfakes Policy
- Nudes & Semi-Nudes Policy
- Searching, Screening & Confiscation Policy

Linked guidance

- Keeping Children Safe in Education
- Online Safety Act 2024
- UKCIS Guidance: Sharing Nudes and Semi-Nudes
- DfE Filtering & Monitoring Standard
- Trust Online Safety Policy
- Trust Behaviour Policies
- Trust Child-on-Child Abuse Policy
- Trust AI & Online Risks Policy

What is cyber bullying?

Cyberbullying is bullying that takes place online or through digital technologies. It is a safeguarding concern and will be managed in line with the Trust's Child Protection & Safeguarding Policy, Behaviour Policy, Child-on-Child Abuse Policy, and Online Safety Policy.

There is legislation in place to help tackle cyber bullying.

- *Section 1 of Malicious Communications Act 1988* it is an offence for any person to send another person a letter, electronic communication or article of any description which intends to cause distress or anxiety to the recipient. This offence carries a maximum sentence of 2 years imprisonment
- *Section 127 of the Communications Act 2003* makes it an offence to transmit any 'message or other matter that is grossly offensive or of an indecent, obscene or menacing character' sent by means of a public electronic communications network. It also makes it an offence to purposefully cause annoyance, inconvenience or needless anxiety by sending an electronic message which is known to be false or persistently send messages to cause annoyance. It can be

difficult to identify the perpetrators but conviction for this offence could result in up to 6 months in prison and a fine
- *Section 89 of the Education and Inspections Act 2006* requires that State schools in England must produce a Behaviour Policy or additional policy which states the strategy for the management of anti-bullying. The Act charges schools with: 'encouraging good behaviour and respect for others on the part of pupils and, in particular, preventing all forms of bullying among pupils'. develop and implement effective anti-bullying strategies. These anti-bullying strategies should also stipulate each organisation's policy relating to the prevention of cyberbullying as well as offline forms of bullying. Anti-bullying and Cyberbullying policies may regulate the behaviour of pupils when they are not in the educational setting or under the control of a teacher to an extent that is reasonable.
- The Online Safety Act 2024 places duties on online platforms to remove harmful content and provides reporting routes for children and schools

Cyberbullying can present in many forms including:

- Communications that are abusive and / or threatening;
- Abusive social media comments / posts;
- Sharing images designed to humiliate a person, including sexual images;
- Spreading false information / rumours;
- Anonymous posting / messaging / trolling;
- Harassment;
- Encouraging self-harm;
- Impersonating someone with the purpose of humiliating or causing distress/harm.
- AI-generated bullying (deepfakes, nudification, impersonation)
- AI-generated sexual imagery of children (illegal CSAM)

Cyberbullying also provides opportunities for group perpetrators to take action, where multiple people are involved in bullying and/or isolating a victim through exclusion. These group dynamics can empower members to carry out and escalate their abusive actions.

The motivations to cyberbully are the same as other forms of bullying however, the online world provides a much wider medium for it to take place. Perpetrators may be motivated by thinking their actions will lead to or retain popularity with others and/or feeling powerful from witnessing the fear/hurt of their victims. They may, but not always, also have low self-esteem and are unable to empathise with their victims.

Patterning

'Patterning', is a term used to describe behaviour where children film child-on-child violent assaults and share the footage on social media platforms. The practice of 'patterning' is specifically carried out with the deliberate intention of embarrassing victims even further by making the video footage across the web. This is an increasing issue.

Patterning is treated as **child-on-child abuse** and must be managed under the Trust Child-on-Child Abuse Policy.

Trolling

Trolling' describes online anti-social behaviours where inflammatory messages are used to deliberately create conflict, hostility and bait others. Trolls, the slang for people who takes this action, provoke disruption by posting on platforms, forums and chat rooms with the intention of causing harm through their inflammatory content. They usually create fake profiles on social media or may steal the identity of another person, in effect posing as them online.

Trolling is a form of cyberaggression, where trolls spread lies and misinformation, name-call with deliberate malicious intent. It is particularly effective on sites which are designed to keep their users anonymous.

Children are taught about cyber bullying and trolling as part of the PSHE/SRE curriculum, as well as through wider opportunities in the curriculum.

Misogyny

Misogynistic online behaviour, including sexist comments, gender-based harassment, sexualised messaging or hostile content targeting girls or women, is recognised as cyberbullying and a safeguarding concern. Misogyny online is treated as harmful sexual behaviour and must be reported to the DSL immediately.

See **child on child abuse** policy

Preventing cyber bulling

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.
- We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. Pupils will be taught how to report concerns using multiple routes (trusted adults, CEOP, Childline, Report Remove).
- We share the National Online Safety poster for online bullying with the children with our families as well as our children (see Appendix 2).
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be covered in class as part of PSHE lessons (or during other curriculum time) and the issue will be addressed in assemblies.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. Resources can be found on National Online Safety to support best practice and address teacher workload.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- Staff must understand their role in monitoring and responding to filtering alerts related to cyberbullying.
- Filtering must not unreasonably restrict teaching and learning (DfE Standard).

Responding to cyber bulling

In relation to a specific incident of cyber-bullying, the schools will follow the processes set out in this policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Staff must remain aware that cyberbullying is bullying.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

When responding to cyberbullying concerns, our schools will:

- Act as soon as an incident has been reported or identified.

- Provide support to those involved (all parties):
    - Reinforce the message to the victim that they should never respond or retaliate to the bullying
    - Support the victim to block and report the accounts
    - Talking through privacy settings to prevent new accounts from making contact;
    - Encourage the person being bullied to keep any evidence (screenshots) of the bullying activity to assist any investigation.
    - Helping those involved to think carefully about what private information they may have in the public domain.
    - Consider the possible impact the cyberbullying content may have had on victims e.g. lowering of self-esteem/self-worth, self-harm and put support in place to address this through internal/external agencies
- Take all available steps where possible to identify the person responsible. This may include:
    - looking at use of the school systems;
    - identifying and interviewing possible witnesses;
    - Contacting the service provider and the police, if necessary.
- Work with the individuals and online service providers to prevent the incident from spreading and assist in removing offensive or upsetting material from circulation. This may include:
    - Support reports to a service provider to remove content if those involved are unable to be identified or if those involved refuse to or are unable to delete content.
    - Confiscating and searching pupils' electronic devices, such as mobile phones, in accordance with the law and the Trust **searching, screening and confiscation policy**
    - Requesting the deletion of locally-held content and content posted online if they contravene school behavioural policies.
- Ensure that sanctions are applied to the person responsible for the cyberbullying; the school will take steps to change the attitude and behaviour of the bully, as well as ensuring access to any additional help that they may need.
- Inform the police if a criminal offence has been committed.
- Report the incident to the Local Authority using Report Racial and Bullying Incidents - KELSI

Remember:

- Cyberbullying is always logged as a safeguarding concern on CPOMS.
- DSLs must review filtering/monitoring alerts for cyberbullying indicators.
- DSLs must consider whether the incident meets the threshold for child-on-child abuse.
- DSLs must consider whether AI-generated content is involved.
- Staff must never ask to see or delete harmful content.
- Staff must use the **Whistleblowing** Policy to report failures in filtering/monitoring.

Logging and dealing with online bullying

The wide range of stages of development and experiences out of school means that there are some children who use racist, discriminatory or derogatory language (including swearing) in an echolalic manner (repeat words they have heard) and these are used out of context i.e. without intent to cause harm. However, this does not mean that the victim in the incident has not been offended – both factors are considered by the staff when logging the incident and responding appropriately.

Monitoring by the senior teams

CPOMS has 2 flags in the Trust schools – contextual or non-contextual so that the senior staff can undertake monitoring of incidents to ensure that these are dealt with swiftly and appropriately.

DSL meetings and/or SLT meetings are used to monitor incidents and discussed. This is then recorded in the meeting minutes and/or on the CPOMS incident so that this is clear and any next steps are identified to ensure that incidents are dealt with fairly and consistently by all staff.

- DSLs must analyse cyberbullying trends termly and report these to LGB in the Heads report
- Governors must receive anonymised cyberbullying data in the Heads report
- Filtering/monitoring logs must be reviewed weekly by Heads and DSLs

Examining electronic devices

Any search must be carried out in line with the **Searching, Screening & Confiscation Policy** and KCSIE 2026

Nude/semi nude images

This section is governed by the Trust **Nudes & Semi-Nudes Policy**. Only a summary is included here.

If a staff member **suspects** a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

If an incident of indecent image sharing is shared by the pupil, then staff must

- Not respond in any way which may make the child feel blamed or shamed;
- Do not ask the child to delete the image or take action to delete it;
- Explain to the child that this needs to be reported and that support will be offered;
- Report the incident to a DSL immediately;
- If viewed, inform the DSL this has happened e.g. if a child shows you an image without detailing its content before sharing it;
- Do not view, copy, print, share or store the image or request the child to share or download the image. This is illegal.

Report Remove (iwf.org.uk) is a tool which young people aged over 13 can ask to have an image removed. This information can be shared with parents/carers to enable the image to be removed where it is illegal.

Generative Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. BA MAT recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully, coerce or intimidate others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes the use of 'nudification' apps or any AI generated bullying or AI generated sexual imagery.

Our schools will treat any use of AI to bully pupils in line with this policy and the behaviour policy.

AI-generated bullying must be logged as a safeguarding concern and managed under the **AI & Online Risks Policy** and **Deepfakes Policy**.

Some terminology which may be used

Some pupils will use terms such as these listed below without having any idea what they mean, or mean to use them in a hurtful way or may mean to use a different word. Use of such terminology will always be explored by staff without assumption.

Staff are advised that if you hear pupils using a term you don't recognise, you can ask them what they mean, and then check to see if the pupil is using the word correctly.

If the term is potentially an offensive one, you can ask them:

- "Do you know that some people might be offended by that word/phrase?"
- "Do you know why it might be a bad idea to say that?"

Language related to cyber-bullying, harassment and cyber crime

Cyber-stalking	Using the internet or text messages to repeatedly harass or bully someone – often using multiple apps and platforms and multiple accounts.
Doxing / Doxxing	Publicly posting someone's private information (e.g. their name, address, place of work or school), usually without their consent. This information might be used to harass the person further.
Dogpiling	When a group of people, usually a large group, target a single person with harassment.
Griefing	Deliberately trying to ruin other people's fun in online games (e.g. blowing up another player's house in Minecraft).
Finsta	'Fake Insta/Fake Instagram' – this may mean a second, private, Instagram account for sharing more personal content with a trusted group of friends, **or** a second Instagram account made to look like another person, either to impersonate them or bully them. This is also known as a 'sock puppet account'.
KYS	Stands for 'kill yourself', used to harass or upset others.
Phishing	A kind of scam where criminals trick targets into giving up personal information (including bank details or account passwords).
Ratio / Ratio'ing	When a negative response to a social media post gets far more positive engagement than the original post.
Troll / Trolling	Deliberately saying hurtful or inflammatory things to get a response from someone, or a group of people.
Sub-tweeting	Negatively talking about someone publicly on social media without tagging them in a post, so the person might not see it. It's most common on X (formerly Twitter) but can happen on other platforms.
Swatting	Calling emergency services (usually the police) and falsely claiming a serious crime is happening at someone else's home (e.g. a bomb threat or a hostage situation), with the intent of police arriving at the person's house. This is done to harass and frighten someone.

Impact assessment

An initial impact assessment has been carried out for this policy and is graded as follows:

A	Positive impact is explicitly intended and very likely
B	**An adverse impact is unlikely, and on the contrary the policy has the clear potential to have a positive impact by reducing and removing barriers and inequalities that currently exist**
C	An adverse impact is unlikely. On the contrary there is potential to reduce barriers and inequalities that currently exist. There is insufficient evidence, however, for this assessment to be made with as much confidence as is desirable
D	Adverse impact is unlikely, but positive impact is also unlikely

E	Adverse impact is probable or certain, since certain groups will be disadvantaged, either proportionately or absolutely, or both. Remedial action is therefore necessary