LLOYD WILLIAMSON
FOUNDATION

The Lloyd Williamson Schools Foundation

CYBER BULLYING AND SOCIAL MEDIA POLICY

2025

Updated by	Aaron Williams	6th June 2025
Due for update	August 2026	

1. Introduction

At Lloyd Williamson Schools, we are committed to fostering a safe, respectful, and inclusive digital environment for all pupils and staff. Cyberbullying and inappropriate use of social media can have serious consequences, affecting mental health, wellbeing, and academic performance. This policy outlines our approach to preventing, identifying, and addressing cyberbullying, ensuring compliance with ISI and DfE regulations.

This policy should be read alongside the following policies:

- Anti-bullying Policy
- Media Policy
- Mobile Device Policy
- Online Safety Policy
- Cyber-security Policy
- E-Safety Policy: Bring Your Own Device (BYOD) Policy for Staff and Visitors
- Safeguarding and Child Protection Policy
- Use of Computers and Internet Access Policy
- Whistleblowing Policy
- Allegations of Abuse Against Staff Policy
- Safer Recruitment Policy
- Staff Code of Conduct
- Behaviour Policy
- Search, Screen and Confiscation Policy

2. Definition of Cyberbullying

Cyberbullying is defined as "the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others" (Belsey). It is an intentional act often carried out repeatedly over time, frequently targeting a victim who struggles to defend themselves. LWSF recognises that cyberbullying can occur inside and outside of school, at any time.

Forms of Cyberbullying

Cyberbullying can involve various electronic media, including:

- Texts, instant messages, emails, or calls on mobile phones.
- The use of mobile phone cameras to cause distress, fear, or humiliation.
- Posting threatening, abusive, sexual, discriminatory, offensive, or humiliating material on websites, including blogs and social networking platforms.
- Hijacking or cloning social media and / or email accounts to impersonate or harm others.

Examples of Cyberbullying

Cyberbullying can manifest in many forms, such as:

- **Cyber-stalking** – persistent harassment or intimidation online.
- **Exclusion or peer rejection** – deliberately excluding someone from online groups or activities.
- **Impersonation** – pretending to be someone else to cause harm.
- **Unauthorised publication of private information or images**.
- **Encouraging derogatory comments** on online platforms.
- **Sharing nude / semi-nude images, upskirting, or sexting**.

3. Social Media Guidelines

For Pupils

- Pupils must use social media responsibly and respectfully.
- Harassment, bullying, or inappropriate content shared online, once reported, will be treated as a serious disciplinary matter under the procedures outlined in both the Anti-bullying Policy and Behaviour Policy (outlined in the form of sanctions).
- Pupils must not engage in online arguments or conflicts that could escalate into bullying.
- Personal information must not be shared publicly or with strangers online.
- Pupils must report any cyberbullying incidents to a trusted adult or the Designated Safeguarding Lead (DSL).

For Staff

- Staff must act professionally when engaging with social media.
- Personal communication with pupils via social media or messaging apps is strictly prohibited.
- Staff must not post or share any content that could compromise the school's reputation.
- Staff must regularly review their privacy settings to prevent unauthorised access.
- Any cyberbullying incidents involving staff must be reported to the Headteacher or DSL. These will be dealt with in line with the school's Allegations of Abuse Against Staff Policy.

4. Prevention of Cyberbullying

To prevent cyberbullying, LWSF implements several measures:

Acceptable Use and Monitoring

- All pupils must follow the school's policy for safe internet and technology use.
- The school's filtering system (FamiSafe) blocks certain sites, and the ICT Lead monitors pupil activity on school devices and platforms.

Consequences for Misuse

Disciplinary action, in line with the Behaviour Policy (For pupils), Allegations of Abuse Against Staff Policy and the Staff Code of Conduct (for staff), may be taken for misuse or attempted misuse of the internet or technology.

Education and Guidance

PSHE lessons provide guidance on safe social networking and cyberbullying, covering:

1. Awareness of the various forms of cyberbullying, its severe consequences, and the school's **zero-tolerance stance**.
2. Guidance on **protecting personal information**, including names, addresses, passwords, and mobile phone numbers.

Mobile Device Policy

LWSF has a clear policy about the permitted use of mobile devices at school and on trips.

5. Procedures for Dealing with Cyberbullying

Report and Document All Incidents

All reports of cyberbullying are taken seriously and must be logged promptly on AIMS. Staff, pupils, or parents can report incidents via email, telephone, or directly in person to the Headteacher and / or Designated Safeguarding Lead (DSL).

- Each report should include details of the incident, individuals involved, the platform where it occurred, and any supporting evidence (such as screenshots).
- A confidential record on AIMS is maintained to track patterns and ensure appropriate follow-up.

Assess the Severity

Once reported, incidents will be assessed to determine the level of harm and whether there is evidence of criminal behaviour.

- **Mild incidents**: such as inappropriate comments or exclusion from online groups, may be handled internally through pastoral support, mentoring and digital education.
- **Serious incidents:** including threats, harassment, sharing explicit content, or identity theft, may require external intervention. In such cases, parents may be informed. The DSL will assess whether to involve social services or police. If the incident includes illegal material (e.g., upskirting, sexting, or online threats), the police will be contacted immediately.

Educate the Perpetrator on Digital Responsibility

LWSF aims to educate pupils and prevent future incidents.

Pupils involved in cyberbullying will be required to attend a restorative justice workshop, learning about the impact of their actions, online ethics, and personal accountability. This may also include discussion about responsible social media use, respectful communication, and consequences for misconduct.

Further disciplinary action, as outlined in the Behaviour Policy, may include restrictions on device access, detentions, or suspensions, depending on the severity.

Ensure the Victim's Online Safety (Adjust Privacy Settings, Block Users)

Protecting the victim is a priority, and immediate steps will be assessed and taken to safeguard their online presence.

- **Adjusting privacy settings** to limit exposure to harmful interactions.
- **Blocking perpetrators** from contacting them on school-monitored platforms.
- **Providing emotional support**, including counselling and pastoral care, to help the victim recover.
- **Monitoring future interactions** to ensure the situation does not escalate or recur.

Electronic Devices: Search and Confiscation

Authority to Search – LWSF has a clear procedure outlined in the Search, Screen and Confiscation Policy.

In response to a cyberbullying allegation, designated staff, authorised by the Headteacher, may search electronic devices (e.g., mobile phones) without parental or pupil consent if they have reasonable grounds to suspect the pupil possesses a prohibited item. The search will follow the Search, Screen and Confiscation Policy.

Examination of Data

If a search reveals a prohibited electronic device, or if staff reasonably suspect it has been used to commit an offence, cause harm, or damage property, the school may examine its data or files if there is good reason (e.g., a cyberbullying allegation). Parental consent may be sought but is not required.

Data Erasure

The school may erase data or files if deemed necessary, unless there are reasonable grounds to suspect the device contains evidence of a criminal offence. In such cases, the files must not be deleted, and the device must be given to the police immediately.

Post-Search Procedures

If a search finds no evidence of an offence, or the police advise they won't investigate, the school may delete files or data and retain the device as evidence of a policy breach. The school may then discipline the pupil under the Behaviour Policy. Safeguarding concerns arising from a search will be handled according to the Safeguarding and Child Protection Policy.

Record Keeping

The school will **maintain records** of all searches, including findings and actions taken, on **AIMS**.

Updated June 2025

Next Update: August 2026