ONLINE SAFETY & SOCIAL MEDIA POLICY 2025–2026

Organisation: Manchester Top Team Youth Project (MTTYP) – Alternative Provision

Reviewed: 1 September 2025 | **Next Review:** 1 September 2026

Designated Safeguarding Lead (DSL): Daryl-Anne Baguley – 07523 983890

Deputy Designated Safeguarding Lead (DDSL): George Smith – 07728 793456

1. Purpose & Policy Statement

MTTYP recognizes that the internet, digital devices, and social media offer valuable learning opportunities, but also present potential safeguarding risks to young people.

This policy sets out clear standards to safeguard students and staff online, ensuring compliance with *Keeping Children Safe in Education (KCSIE)*, the *Prevent Duty*, and UK GDPR guidelines. It applies to all staff, sessional mentors, tutors, volunteers, and students accessing digital technology across MTTYP settings.

2. Technical Safeguards: Filtering & Monitoring Systems

In accordance with statutory KCSIE standards, MTTYP enforces robust filtering and monitoring protocols across all digital infrastructure:

- **Appropriate Filtering:** All MTTYP internet connections, Wi-Fi networks, laptops, tablets, and mobile hardware are protected by age-appropriate broadband and DNS filtering systems. This blocks access to illegal content, violent extremism, terrorism, pornography, gambling, self-harm material, and unapproved social networking platforms.
- **Active Monitoring & Flagging:** Monitoring software tracks device usage on MTTYP hardware to identify search terms, typed text, or accessed URLs related to radicalisation, child sexual exploitation (CSE/CCE), suicide/self-harm, cyberbullying, or illegal activity.
- **System Audits & Response:** The DSL team receives automated alerts for critical flags. The effectiveness of filtering and monitoring software is audited termly by Executive Management to ensure system integrity.

3. Professional Digital Boundaries for Staff

To maintain professional safety, staff must strictly adhere to digital communication rules:

- **Official Channels Only:** All digital communication with students or parents/carers must occur strictly through official MTTYP-issued phone lines, email addresses, or approved management platforms.
- **Personal Social Media & Messaging:** Staff must **never** connect with, "friend", follow, or direct-message current students on personal social media accounts (e.g., Instagram, TikTok, Snapchat, Facebook, WhatsApp).

- **Gaming & Private Platforms:** Staff are strictly prohibited from playing online video games or joining private chat channels with students using personal accounts.
- **Personal Media Capture:** Staff must never use personal mobile phones or cameras to capture images or videos of students. All media must be recorded on MTTYP equipment in line with our *Photography & Media Policy*.

4. Student Digital Expectations & Safety Education

- **Acceptable Use Agreement:** Students sign a digital Acceptable Use Agreement during onboarding, agreeing to use MTTYP digital devices responsibly and for approved educational tasks.
- **Preventing Digital Harassment:** Online bullying, harassment, sending non-consensual intimate images (sexting/upskirting), or sharing hate speech will be treated as severe safeguarding breaches and escalated under our *Anti-Bullying & Peer-on-Peer Abuse Policy*.
- **Online Safety Curriculum:** Digital literacy, online grooming awareness, privacy management, and critical evaluation of online content (misinformation/extremism) are integrated into 1:1 mentoring and personal development sessions.

5. Responding to Online Incidents & Escalation

1. **Incident Triage:** Any staff member informed of an online safety concern, digital boundary breach, or harmful content exposure must immediately notify the **DSL (Daryl-Anne Baguley)** or **DDSL (George Smith)**.
2. **Evidence Preservation:** Staff must preserve digital evidence (e.g., taking screenshots of messages or URLs) without forwarding or distributing explicit/illegal images.
3. **Statutory Escalation:** Severe online safety incidents (e.g., child sexual abuse material, grooming, radicalisation, or extortion) will be referred immediately to the **Police / CEOP**, **Local Authority Children's Social Care**, or the **Prevent Team**.