

Here is the complete, fully updated **Data Protection & GDPR Policy 2025–2026 / 2026–2027**, incorporating clear statutory retention schedules for student safeguarding files (retained until age 25) and explicit protocols for responding to Subject Access Requests (SARs) within 30 days.

DATA PROTECTION & GDPR 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. Policy Statement & Legal Framework

MTTYP is committed to protecting the privacy, confidentiality, and data rights of all students, parents/carers, staff, sessional mentors, and stakeholders.

This policy ensures compliance with:

- *UK General Data Protection Regulation (UK GDPR)*
- *Data Protection Act 2018 (DPA 2018)*
- *Education (Pupil Information) (England) Regulations*
- *Keeping Children Safe in Education (KCSIE)*

MTTYP processes personal and special category data lawfully, fairly, and transparently, maintaining robust technical and organizational security measures.

2. Principles of Data Protection

MTTYP adheres strictly to the core UK GDPR principles:

1. **Lawfulness, Fairness & Transparency:** Data is collected lawfully and used in ways individuals reasonably expect.
2. **Purpose Limitation:** Collected strictly for specified, explicit alternative provision and safeguarding purposes.
3. **Data Minimisation:** Adequate, relevant, and limited to what is necessary.
4. **Accuracy:** Kept accurate and, where necessary, up to date.
5. **Storage Limitation:** Kept in a form permitting identification for no longer than necessary.
6. **Integrity & Confidentiality:** Processed securely to protect against unauthorized access, loss, or damage.

3. Handling Special Category & Safeguarding Data

- **Special Category Data:** Information regarding health, EHCP status, ethnicity, religious beliefs, or criminal allegations/convictions is handled under additional strict safeguards.
- **Safeguarding Overrides Confidentiality:** While data protection rules are strictly enforced, **data protection law is not a barrier to sharing information where there are child protection concerns.** In line with *KCSIE* and *Working Together to Safeguard Children*, staff will share relevant personal data with Social Care, Police, or the LADO without consent if a child is at risk of harm.

4. Statutory Data Retention Schedules

MTTYP maintains clear retention timeframes in accordance with statutory guidelines and Information and Records Management Society (IRMS) standards:

Safeguarding & Child Protection Records

— Retained until the pupil reaches the age of 25 (or 75 years for Care Leavers)

General Pupil Educational Records

— Retained for 6 years after the pupil leaves MTTYP provision

Personnel & SCR Records

— Retained for 6 years post-employment (DBS numbers deleted as appropriate)

Financial & Grant Audit Records

— Retained for 6 years plus current financial year

- **Safeguarding Files:** Confidential safeguarding files, body maps, and incident logs are stored separately from general educational files and are **retained until the young person reaches their 25th birthday** (or transferred securely to the commissioning school/local authority upon exit).
- **Secure Destruction:** Digital files are permanently erased, and physical files are confidentially shredded upon reaching the retention limit.

5. Subject Access Requests (SARs) & Data Rights

Individuals (data subjects) have the right to access personal data held about them by MTTYP.

- **Submitting a Request:** SARs can be made verbally or in writing to Executive Management or the DSL.
- **30-Day Statutory Deadline:** MTTYP will verify the identity of the requester and respond in full **within 30 calendar days** (one calendar month) of receipt.
- **Exemptions & Safeguarding Redactions:** Information will be redacted or withheld if disclosure would cause serious harm to the physical or mental health of the pupil or another individual, or if it relates to ongoing child protection/police investigations.

6. Data Security & Breach Reporting

6.1 Technical & Organizational Controls

- Electronic student data is encrypted and accessible only via secure, role-restricted MTTYP accounts.
- Physical records are stored in locked cabinets within secured spaces.
- Personal email accounts or unencrypted personal USB drives must **never** be used to store or transmit student data.

6.2 Data Breach Procedure

- Any suspected or confirmed personal data breach must be reported immediately to Executive Management.
- If a breach poses a risk to the rights and freedoms of individuals, MTTYP will notify the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware