The Fatherhood Project

Data Protection & UK GDPR Policy

Youth & Minors Protection

Document Version: 1.0
Approved by: Board of Directors
Date of Next Review: May 2027
Data Protection Officer (DPO): [Insert Name]

1. Introduction & Scope

The Fatherhood Project collects and processes personal data relating to minors (aged 11–18) to deliver safe mentorship, monitor crime-prevention outcomes, and maintain safeguarding standards. We are committed to processing all data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Because we work with minors, we operate under a strict "Safety-First" data framework, recognizing that the data we hold is highly sensitive.

2. What Data We Collect & Our Legal Basis

We collect only the minimum necessary data required to keep young people safe and track their progress. This includes:

Personal Data: Names, dates of birth, home addresses, and emergency contact details.

Special Category Data: Ethnicity (for EDI monitoring), school attendance/exclusion history, and details regarding risk of criminal exploitation or Youth Justice Service involvement.

Our Legal Basis for Processing:

Consent: Explicit, written consent is obtained from a parent or legal guardian before a minor joins our programme (and from the young person themselves where age-appropriate).

Vital Interests / Legal Obligation: In emergency scenarios where a minor is at risk of harm, data may be shared with emergency services or safeguarding teams without prior consent.

3. How We Securely Store the Data of Minors

To match the standards of statutory bodies, The Fatherhood Project enforces a strict digital-first, zero-paper protocol for youth data:

A. Secure Cloud Infrastructure

No Paper Records: Physical registration forms are scanned into our secure system immediately and then securely shredded using a cross-cut shredder. No paper records containing minors' names or addresses are kept in local offices or transported by mentors.

Encrypted Central Database: All youth data, session logs, and mentor matchings are stored on a GDPR-compliant, encrypted central database (e.g., Upshot, Views, or a secure, restricted-access corporate OneDrive/Google Workspace environment).

Two-Factor Authentication (2FA): Access to the database requires a secure password and mandatory 2FA (a code sent to a mobile device).

B. Strict Access Control (The "Need to Know" Principle)

The CEO and Management Committee have full access to records for compliance and reporting.

Frontline Mentors are only granted access to the specific details of the minor they are actively mentoring. They cannot view the records of other youth in the project.

Device Security: All devices (laptops, mobiles) used by managers and mentors to access project data must be password/biometric-protected and encrypted.

C. Safe Communication Protocols

No Messaging of Sensitive Data: Staff and mentors are strictly prohibited from sharing full names, addresses, or sensitive case notes of minors over standard SMS, personal WhatsApp, or social media.

Anonymisation: For general internal communication or committee meetings, minors are referred to by an ID number or initials only (e.g., "Youth JW-01").

4. Data Retention & Secure Disposal

Retention Period: We retain youth records for 6 years after they leave the project or turn 18, in alignment with statutory safeguarding and limitation guidelines.

Secure Deletion: Once the retention period expires, digital records are permanently wiped from the cloud database and servers using secure digital overwriting tools.

5. Rights of the Minor and Guardians

Under UK GDPR, parents/guardians (and minors, depending on understanding) have the right to:

- Request a copy of the data we hold about them (Subject Access Request).
- Request that inaccurate data be corrected.
- Request that their data be deleted (where it does not conflict with our legal safeguarding duties).

6. Data Breach Procedure

In the unlikely event of a data breach (e.g., a manager's laptop is stolen or an unauthorized person accesses the database):

- The Data Protection Officer will immediately lock down the affected accounts.
- The breach will be investigated and logged.
- If the breach poses a risk to the rights and freedoms of the minor, we will notify the Information Commissioner's Office (ICO) and the affected parents/guardians within 72 hours.

Signed on behalf of the Board:

[Your Name], Chief Executive Officer
Date: [Insert Date]