DATA PROTECTION/GDPR POLICY

2025 – 2026

POLICY STATUS: **Statutory**

POLICY CYCLE: **Annually**

OWNER: **Urban Judge**

PERSON RESPONSIBLE: **Data Protection Lead**

APPROVED BY: **Advisory Board**

VERSION CONTROL

Adoption: **January 2025**

Latest Review: **August 2025**

Next Review: **September 2026**

Contents

1. Introduction

This policy sets out Youth Television CIC known as 'YouthTV''s approach to data protection and privacy, ensuring compliance with the UK GDPR, the Data Protection Act 2018, and all other relevant legislation.

It applies to all YouthTV staff, directors, volunteers, advisors and anyone working on behalf of YouthTV.

Its aims are to:

- Protect the rights, safety, and privacy of individuals.
- Maintain the trust and confidence of service users, partners, funders, and stakeholders.
- Prevent reputational and legal harm to YouthTV.
- Ensure that personal data is handled lawfully, fairly, securely, and only for legitimate purposes.

The consequences of mishandling personal data can be severe, including:

- Harm or distress to individuals.
- Financial penalties from the ICO (up to £17.5m or 4% of annual turnover).
- Loss of public trust and reputational damage.

2. Roles and Responsibilities

- Overall Responsibility: YouthTV's CEO (Urban Judge) holds ultimate accountability for compliance.
- Data Protection Lead: Ryan Harris (Advisory Board) oversees policy implementation and advice.
- Senior Leadership:
    - Krish Gupta – Chief Operating Officer (Operational Compliance)
    - Ashton Williamson – Chief Broadcasting and Content Officer (Brand and Compliance)
- All YouthTV Members: Everyone handling personal data must:
    - Understand their obligations under this policy.
    - Use personal data only for legitimate business purposes.
    - Report any suspected breaches immediately.

3. Definitions

Personal Data	Any information that can identify a living person, e.g. name, email, phone number, address, video footage, or ID number.

Special Category Data	Information requiring extra protection (UK GDPR Art. 9), such as racial/ethnic origin, religious beliefs, sexual orientation, health data, biometric data.
Processing:	Any action performed on data (collecting, storing, sharing, deleting)
Data Subject:	The person whose data we process.
Controller:	YouthTV, when deciding how data is processed.
Processor:	Third parties processing data on YouthTV's behalf (e.g., BreatheHR, Xero, Microsoft 365, Canva).
Informed Consent:	The clear, unambiguous agreement of the Data Subject to data processing.

4. Data Protection Prinicples

YouthTV commits to **UK GDPR Article 5** principles:

1. **Lawfulness, fairness, transparency** – clear reasons for processing data.
2. **Purpose limitation** – only collect for specific, stated purposes.
3. **Data minimisation** – only keep what's necessary.
4. **Accuracy** – keep data up-to-date.
5. **Storage limitation** – keep data only as long as needed.
6. **Integrity and confidentiality** – protect against loss, damage, or unauthorised access.

Example:
If a volunteer collects sign-up forms for a YouthTV filming project, they must store them securely, use them only for the stated project, and delete them when no longer required.

5. Data Accurancy & Updating Records

YouthTV is committed to ensuring that all personal data we hold is accurate, complete, and up to date. We recognise that inaccurate or outdated information can lead to poor decision-making, breaches of trust, and potential harm to individuals. As part of our compliance with the UK GDPR and Data Protection Act 2018, we will take reasonable steps to check the accuracy of data at the point of collection and at regular intervals thereafter. Individuals have the right to request corrections to any inaccuracies, and YouthTV will respond to such requests promptly, typically within one calendar month.

We will maintain clear procedures for updating records, and wherever possible, updates will be made directly by the individual concerned, such as through secure online forms or verified written communications. This ensures that personal details like addresses, contact numbers, or emergency contact information remain correct and reduce the likelihood of misdirected communications.

Example: If a YouthTV workshop participant moves to a new address and updates their details via our online registration system, the administrator will verify and update their information in Microsoft 365, ensuring that all production and outreach teams use the correct contact details in future communications.

6. Transparency & Consent

YouthTV will be transparent with individuals about why we are collecting their personal data, how it will be used, and who it may be shared with. This is communicated through privacy notices, consent forms, and verbal briefings where appropriate. Consent will be clear, specific, and informed, avoiding any pre-ticked boxes or vague terms. For sensitive personal data — such as medical information, special educational needs, or safeguarding concerns — explicit consent will always be sought unless there is another lawful basis for processing.

Wherever possible, consent will be recorded and stored securely within YouthTV systems. Individuals will also be informed of their right to withdraw consent at any time without detriment. We will not assume consent for purposes that go beyond what was initially agreed.

Example: When YouthTV records interviews for a community documentary, each participant is given a consent form explaining exactly how the footage will be used (e.g., on YouTube, in educational resources, or in promotional materials). If a participant later decides they do not want their segment to be shared online, YouthTV will take reasonable steps to edit or remove it from future public use.

7. Security of Data and ICT Systems

YouthTV applies robust technical and organisational measures to keep personal data secure. All data must be stored within secure, approved platforms such as BreatheHR, Xero, Microsoft 365, and Canva. These platforms are to be used strictly for YouthTV-related work and must not be used for personal projects or non-work purposes. When using personal devices for YouthTV work, members must ensure they are password-protected, encrypted, kept up-to-date with security patches, and locked when not in use.

The security of ICT systems and data storage is governed in conjunction with YouthTV's ICT Acceptable Use Policy, which sets out clear rules for the safe, lawful, and responsible use of devices, software, and online accounts. All members must familiarise themselves with this policy and comply with its requirements when handling personal data or accessing YouthTV systems.

We prohibit the storage of YouthTV personal data on unsecured or unauthorised devices. Access permissions are granted only to those who require it for their role, and accounts must be protected with strong passwords and, where possible, multi-factor authentication. All staff, volunteers, and advisors are responsible for reporting any potential security risks immediately.

Example: A volunteer accessing BreatheHR from a personal tablet to update event attendance must ensure they log out fully after use, avoid downloading participant data to their device, and store all files on YouthTV's secure Microsoft 365 platform. If their tablet is lost or stolen, they must notify the CEO immediately so that remote access can be blocked.

8. Data Retention and Secure Disposal

YouthTV will retain personal data only for as long as necessary to fulfil the purposes for which it was collected, including legal, contractual, or reporting obligations. Retention periods are defined in our Data Retention Schedule, which sets out how long we keep different categories of data and the secure disposal methods we use. Once the retention period has expired, data will be deleted, shredded, or anonymised to prevent identification.

Physical records containing personal data will be stored in locked cabinets or secure storage areas and destroyed via cross-cut shredding or certified confidential waste disposal. Digital files will be securely deleted using data wiping tools to ensure they cannot be recovered.

Example: After a funded film project ends, YouthTV will anonymise statistical data for reporting to funders but will delete all participant consent forms and identification documents from Microsoft 365 after the agreed retention period, ensuring compliance with the Data Protection Act 2018.

9. Data Sharing and Disclosure

YouthTV will only share personal data when there is a lawful basis for doing so, such as fulfilling a contract, meeting a legal requirement, or with the individual's explicit consent. Any sharing of personal data will be proportionate, limited to what is strictly necessary, and transmitted securely.

Where third parties process data on behalf of YouthTV, we will have a written data processing agreement in place to ensure they meet the same data protection standards. We will not sell or rent personal data to any organisation.

Example: If YouthTV partners with a local college to deliver a training programme, participant names, contact details, and learning support needs may be securely shared with the college via a password-protected Microsoft 365 folder. The college will be contractually required to delete or return the data once the programme ends.

10. Data Breach Management

Any YouthTV member who suspects a data breach must report it immediately to the CEO and the Data Protection Lead. A breach includes unauthorised access, accidental loss, destruction, or disclosure of personal data. All breaches will be recorded in the Data Breach Log, investigated promptly, and, if necessary, reported to the Information Commissioner's Office (ICO) within 72 hours.

If the breach poses a high risk to individuals, YouthTV will notify the affected individuals without undue delay, explaining the nature of the breach, what data was affected, and the steps they should take to protect themselves. Preventative actions will be taken to reduce the risk of future incidents, and staff responsible for breaches may face disciplinary action.

Example: If an advisor accidentally sends a participant list with phone numbers to the wrong email address, they must immediately contact the unintended recipient requesting deletion, inform the CEO, and complete a breach report. The Data Protection Lead will then assess whether the ICO needs to be notified and may arrange additional staff training on email security.