Croydon Youth Theatre Organisation (CYTO)

Data Protection and GDPR Policy

Approved by: CYTO Board of Trustees
Approval Date: Nov 26
Review Date: Nov 27

1. Purpose

CYTO is committed to protecting the privacy, safety, and rights of all individuals whose personal data we process. This policy explains how CYTO collects, stores, uses, shares, and protects personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable legislation.

As a youth organisation, CYTO recognises the importance of safeguarding children and young people's personal information and takes additional care when processing data relating to individuals under 18.

This policy applies to:

- Members and participants (past and present)
- Parents, carers and guardians
- Staff, freelancers and volunteers
- Trustees and committee members
- Stakeholders
- Contractors
- Audience members
- Individual donors, benefactors and supporters
- Individuals engaging with CYTO online or through social media

2. Data Controller

CYTO is the data controller responsible for determining how personal data is collected and used.

Data Protection Lead: Andrew McPherson
Contact Email: andrewmcpherson@cyto.org.uk

CYTO is registered with the Information Commissioner's Office (ICO) as a data controller.

ICO Registration Number: ZA099535

3. Principles of Data Protection

CYTO processes personal data in accordance with the following principles:

- Data is processed lawfully, fairly, and transparently
- Data is collected for specified, explicit, and legitimate purposes
- Data collected is relevant and limited to what is necessary
- Data is accurate and kept up to date
- Data is retained only for as long as necessary (up to seven years)
- Data is processed securely and confidentially
- CYTO takes responsibility for demonstrating compliance

4. Types of Personal Data We Collect

Depending on involvement with CYTO, we may collect and process:

4.1 Member and Participant Information

- Names
- Dates of birth
- Home addresses
- Parent/carer contact details
- Telephone numbers
- Email addresses
- Emergency contact information
- Attendance records
- Participation records
- Casting and performance information

4.2 Special Category Data

CYTO may collect certain special category data where necessary for safeguarding, accessibility, health, or duty of care purposes.

This may include:

- Medical information
- Allergy information
- Access requirements
- Disability information
- Dietary requirements
- Relevant safeguarding information
- Diversity Monitoring information (usually for funding reports)
- Photo, video and voice recording consent information.
- Descriptions of financial situation (for discounted and bursary places)

We process special category data under:

- Article 9(2)(a) UK GDPR – explicit consent
- Article 9(2)(c) UK GDPR – vital interests
- Article 9(2)(g) UK GDPR – safeguarding and substantial public interest where applicable

Special category data is accessed only by authorised individuals who require the information to support safeguarding, safety, or operational responsibilities.

4.3 Staff and Volunteer Information

- Names
- Dates of birth
- Home addresses
- Contact details
- DBS status where applicable
- Training records
- Telephone numbers
- Email addresses
- Emergency contact information
- Attendance records
- Role and availability information
- Medical information
- Allergy information
- Access requirements
- Disability information
- Dietary requirements
- Diversity Monitoring information (usually for funding reports)
- Photo, video and voice recording consent information.

4.4 Marketing and Communications Data

- Newsletter subscriptions
- Mailing preferences
- Records of communication consent

4.5 Website and Social Media Data

CYTO may collect limited information through interactions with our website and official social media accounts, including:

- Names and usernames
- Public comments or messages
- Social media interactions (likes, comments, tags, follows)
- Photographs or media shared with consent

Personal data shared via social media is handled in accordance with this policy and CYTO's safeguarding procedures. Personal data relating to children and young people will not be shared publicly without appropriate consent.

CYTO staff and volunteers must not make or accept personal social media contact with young people through private accounts, in line with the organisation's safeguarding policy.

Where CYTO engages with young people through official CYTO social media accounts, we take additional care to ensure:

- CYTO avoids direct private messaging with young people through social media wherever possible
- Where communication is necessary, it takes place through official organisational channels with appropriate oversight
- Communication remains appropriate and transparent
- Parent/carer consent is obtained where necessary

- Interactions are monitored by authorised adults
- No unnecessary personal data is collected or retained

5. Lawful Bases for Processing

CYTO processes personal data using the lawful bases below.

Activity	Lawful Basis
Membership administration	Contract
Session participation records	Contract
Emergency contacts and medical information	Vital interests / Legal obligation
Safeguarding records	Legal obligation / Substantial public interest
Volunteer and staff administration	Contract / Legal obligation
Email newsletters and marketing	Consent
Photography and media use	Consent
Financial and accounting records	Legal obligation
Operational improvement and planning	Legitimate interests
Website and social media engagement	Legitimate interests / Consent

Where CYTO relies on legitimate interests, we ensure that our interests in operating and improving CYTO do not override the rights and freedoms of individuals. Appropriate balancing assessments are carried out where required.

Consent is requested separately for optional activities such as:

- Marketing communications
- Photography and video use
- Social media publication
- Promotional materials

Participation in CYTO activities is not conditional upon consenting to optional marketing or media processing.

In certain safeguarding circumstances, CYTO may process or share personal data without consent where necessary to protect a child, young person, or vulnerable individual from harm or where required by law.

6. Children’s Data

CYTO recognises that children and young people require additional protection regarding their personal data.

Parental, carer or guardian consent will be obtained before collecting or using a child’s personal data, particularly in relation to:

- Media and photography
- Social media engagement
- Marketing communications
- Medical and emergency information
- Diversity monitoring

We take additional safeguards when handling children's data and ensure information is only accessible to authorised individuals with a legitimate need to know.

7. How We Store and Protect Data

CYTO only collects personal data that is necessary for specific operational, safeguarding, or legal purposes. We avoid collecting excessive information and regularly review forms, records, and processes to ensure only essential data is requested and retained.

CYTO takes appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse, or disclosure.

These measures include:

- Password-protected systems and accounts
- Two-factor authentication where available
- Secure cloud storage
- Restricted access to personal data
- Secure disposal and shredding of paper records
- Regular review of stored information
- Appropriate use of BCC in group emails
- Verification of recipients before sending emails containing personal data
- Secure handling of attachments and sensitive information

Physical Records

Printed records containing personal or sensitive information, including emergency contact folders and medical forms, must:

- Be stored in locked drawers, cabinets, or secure offices when not in use
- Only be accessible to authorised staff or volunteers
- Never be left unattended in public or shared spaces
- Be transported securely when required for events or productions

CYTO recognises the heightened safeguarding importance of printed emergency contact information during productions and events, particularly where young people may pass through backstage or office areas.

Personal or safeguarding information should not be discussed in public, backstage, or shared areas where it may be overheard.

Access to safeguarding and medical information is limited strictly to individuals with a legitimate safeguarding or operational need to know.

"Authorised adults" refers to DBS-checked staff, trustees, volunteers, or contractors approved by CYTO to access personal data as part of their role.

Personal data should only be accessed on personal devices where authorised and necessary. Any personal data stored temporarily on personal devices must be password protected and deleted promptly after use. Registers, safeguarding records, and contact lists should not be permanently stored on personal devices or unsecured downloads folders.

8. Third-Party Processors and Data Sharing

CYTO may use trusted third-party providers to support administration and communication.

These may include:

- POWR
- Mailchimp
- Microsoft Office 365
- Payment processors (Stripe & PayPal)
- Fundraising websites (Easy Fundraising and Peoples' Fundraising)
- Cloud storage providers

These organisations act as data processors on behalf of CYTO and are required to process data securely and lawfully.

Online forms used by CYTO are designed to collect only necessary information and are secured through reputable third-party providers with appropriate data protection measures.

Some data may be processed or stored outside the United Kingdom. Where this occurs, CYTO ensures appropriate safeguards are in place, such as:

- UK adequacy regulations
- International Data Transfer Agreements (IDTAs)
- Standard Contractual Clauses (SCCs)

CYTO does not sell personal data.

Personal data may be shared where required:

- For safeguarding purposes
- To protect vital interests
- To comply with legal obligations
- With emergency services where necessary

9. Data Retention

CYTO retains personal data only for as long as necessary for the purpose for which it was collected.

Retention periods may include:

Data Type	Retention Period
Current member records	Duration of membership
Former participant records	Up to 7 years after leaving, unless further consents are sought
Safeguarding records	In accordance with safeguarding guidance and risk assessment, potentially until age 25 or longer where necessary
Medical and emergency information	Current membership period only unless required for safeguarding
Mailing list subscriptions	Until consent is withdrawn or after 10 years of inactivity
Financial records (including Payroll)	6 years
Staff and volunteer records	Up to 6 years after involvement ends
Media consent forms	Until consent withdrawn or material retired

Data that is no longer required will be securely deleted, anonymised, or destroyed.

10. Photography, Video, and Social Media Use

CYTO's website may use cookies or analytics tools to understand website usage and improve user experience. Further details are provided in the website cookie notice where applicable.

CYTO may use photographs, recordings, or videos for:

- Production promotion
- Marketing materials
- Social media content
- Funding applications
- Press releases
- Website content

Separate consent will be requested for:

- Internal use
- Website publication
- Social media publication
- Press or promotional use

Consent may be withdrawn at any time.

Historical production photography already included in printed programmes, archived publicity materials, or past social media posts may not always be removable retrospectively, though CYTO will take reasonable steps where feasible.

CYTO will take reasonable steps to ensure images and media are used appropriately and safely, particularly where children and young people are involved.

11. Individual Rights

Under UK GDPR, individuals have the right to:

- Be informed about how their data is used
- Access their personal data
- Request correction of inaccurate data
- Request deletion of personal data where appropriate
- Restrict processing
- Object to certain processing activities
- Withdraw consent at any time
- Request data portability where applicable
- Lodge a complaint with the Information Commissioner's Office (ICO)

Requests relating to personal data should be directed to the Data Protection Lead.

CYTO will normally respond to Subject Access Requests within one calendar month in accordance with UK GDPR requirements.

Further information about data protection rights can be found via the ICO:

Information Commissioner's Office (ICO) - https://www.ico.org.uk

12. Data Breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Any suspected data breach must be reported immediately to the Data Protection Lead.

CYTO will:

- Investigate all reported breaches
- Take immediate steps to minimise risk
- Record breach details and actions taken
- Notify the ICO within 72 hours where legally required
- Inform affected individuals where there is a high risk to rights and freedoms

13. Staff and Volunteer Responsibilities

All staff, volunteers, trustees, and contractors handling personal data must:

- Follow this policy
- Keep personal data confidential
- Use data only for authorised purposes
- Report data breaches immediately
- Follow safeguarding and social media procedures
- Complete any required data protection training

Failure to comply with this policy may result in disciplinary action.

CYTO aims to ensure that staff and volunteers with access to personal data receive appropriate data protection and safeguarding guidance.

Staff and volunteers handling personal data may be required to confirm that they have read and understood this policy.

14. Review and Monitoring

This policy will be reviewed annually or sooner if:

- Legal requirements change
- Organisational practices change
- Significant incidents occur
- New systems or technologies are introduced

15. Related Policies

This policy should be read alongside:

- Safeguarding Policy
- Codes of Conduct
- Child Protection Policy

16. Contact Information

For questions about this policy or personal data, please contact:

Data Protection Lead: Andrew McPherson
Email: andrewmcpherson@cyto.org.uk
Postal Address: CYTO, The Shoestring, Oakley Rd, South Norwood, SE25 4XG

Signatures



_____

Andrew McPherson
Artistic Director and Data Protection Lead.



_____

Anna Shields
Co-chair of Board of Trustees