



GDPR and Data Protection Policy

Version Number	Changed By	Changes Made	Date Modified	Next Review Date
v.1	Dominique Gorman (Office Manager)	Edited all areas to bring up to date	19/05/2026	19/05/2026 (annual review)



YOUNG LEWISHAM PROJECT

Introduction:

The Young Lewisham Project is committed to delivering high-quality services in a safe, secure, and legally compliant way. This includes protecting all personal data we collect, use, store, and share, and ensuring transparency in how personal information is handled.

We recognise our responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and related legislation. We are committed to handling personal data lawfully, fairly, securely, and transparently at all times.

This policy applies to all employees, trustees, volunteers, contractors, agency workers, and third parties working on behalf of The Young Lewisham Project.

Aims:

Our aims are to:

- Ensure compliance with the UK GDPR and Data Protection Act 2018 (DPA 2018).
- Promote good practice in handling personal data.
- Safeguard the privacy rights of all individuals whose personal data we process.
- Provide clear guidance to staff, trustees, volunteers, and third parties on handling personal data lawfully and securely.

This policy applies to all personal data held by the young Lewisham Project, regardless of the format, including electronic records, paper files, photographs, video recordings, CCTV footage, emails and verbal records.

Definitions:

- **Personal Data:** Any information relating to an identifiable individual, such as name, contact details, ID number, or online identifier.
- **Special Category Data:** Sensitive data requiring extra protection, e.g., racial or ethnic origin, health, sexual orientation, political opinions, or biometric data.
- **Data Subject:** The individual whose personal data is processed.
- **Data Controller:** The Young Lewisham Project, which determines how and why personal data is processed.
- **Data Processor:** Any third party processing personal data on behalf of The Young Lewisham Project.
- **Processing:** Any operation performed on personal data, including collection, storage, use, sharing, or disposal.
- **Data Breach:** Any accidental or unlawful loss, destruction, alteration, disclosure, or access to personal data.



Legislation and Guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR), where applicable
- Human Rights Act 1998
- Freedom of Information Act 2000 (where applicable)
- Information Commissioner's Office (ICO) guidance and codes of practice
- ICO's Code of Practice for CCTV and surveillance

Roles and Responsibilities:

Governing Body (Trustees)

The Board of Trustees is ultimately responsible for ensuring that The Young Lewisham Project complies with data protection legislation. Trustees will:

- Approve and review this policy regularly
- Ensure appropriate resources are available for compliance
- Monitor organisational data protection risks

Data Protection Officer (DPO)

The organisation will appoint a designated Data Protection Lead (or Data Protection Officer where legally required) responsible for:

- Monitoring compliance with data protection legislation
- Advising staff and trustees on data protection matters
- Managing data breaches and Subject Access Requests
- Acting as the main point of contact with the ICO
- Maintaining records of processing activities where required

Managers

Managers are responsible for:

- Ensuring staff follow this policy
- Identifying and managing data protection risks
- Ensuring personal data is processed securely within their area of responsibility



All Staff, Volunteers, and Contractors:

All staff, volunteers, and contractors must:

- Process personal data only in line with organisational procedures
- Keep personal information secure and confidential
- Report data breaches or concerns immediately
- Complete mandatory data protection training
- Only access personal data necessary for their role

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

Data Protection Principles:

We comply with the six GDPR principles. Personal data must be:

1. Processed lawfully, fairly, and transparently
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Stored no longer than necessary
6. Processed securely using appropriate technical and organisational measures.

We are also accountable for demonstrating compliance with these principles.

Collecting and Processing Personal Data:

We process data only when we have a lawful basis, which may include:

- Consent
- Performance of a contract
- Compliance with a Legal obligations
- Protection Vital interests
- Public interest or legitimate interests

Where special category data is processed, we will identify an additional lawful condition under Article 9 UK GDPR and Schedule 1 of the data Protection Act 2018. also meet additional conditions under UK GDPR/DPA 2018.



YOUNG LEWISHAM PROJECT

Where consent is relied upon:

- Consent must be freely given, specific, informed, and unambiguous
- Individuals may withdraw consent at any time
- Records of consent will be maintained.

Children and Young People's Data

As we work with children and young people, we recognise the need for enhanced protections.

We will:

- Process children's data fairly and transparently
- Use age-appropriate language in privacy notices where appropriate
- Obtain Parental or guardian concerns are managed in line with safeguarding legislation and guidance.

Information may be shared without consent where there is a lawful safeguarding reason to do so.

We will provide clear privacy notices explaining:

- What personal data we collect
- Why we collect it
- How it will be used
- Who it may be shared with
- How long it will be retained
- Individuals right under data protection law
- How to complain to the ICO

Privacy notices will be available to staff, volunteers, service users, parents/carers, and other relevant individuals.



Individual Rights

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making and profiling

Requests relating to these rights should be made to the Data Protection Lead.

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO).

Subject Access Requests (SARs)

Individuals may request access to their personal data verbally or in writing.

The organisation will:

- Respond without undue delay and within one calendar month
- Verify identity before releasing information where necessary
- Provide information free of charge unless requests are excessive or unfounded
- Keep records of requests and responses

The response period may be extended by up to two additional months for complex requests, in accordance with UK GDPR requirements.



Information Sharing

Personal data will only be shared where:

- There is a lawful basis to do so
- Sharing is necessary for safeguarding or protection purposes
- Sharing is required by law
- Sharing is necessary for service delivery
- Appropriate contracts or data-sharing agreements are in place

We will never sell personal data.

Where third-party processors are used, we will ensure contracts meet UK GDPR requirements.

International Data Transfers

Personal data will not normally be transferred outside the UK unless appropriate safeguards are in place in accordance with UK GDPR requirements.

Safeguards may include:

- UK adequacy regulations
- International Data Transfer Agreements (IDTAs)
- Other lawful transfer mechanisms recognised under UK GDPR

Data Security

We will implement appropriate technical and organisational measures to protect personal data, including:

- Password protection and multi-factor authentication where appropriate
- Encryption of devices and sensitive data
- Secure storage of paper records
- Role-based access controls
- Confidential disposal of records
- Secure backup systems
- Cybersecurity and anti-virus protections



Staff must:

- Lock screens when away from devices
- Avoid sharing passwords
- Use secure methods when sending personal data
- Report lost or stolen devices immediately

Data Retention and Disposal

Personal data will only be retained for as long as necessary for the purposes for which it was collected, including legal, safeguarding, financial, and operational requirements.

Retention periods will be set out in a separate retention schedule.

When data is no longer required, it will be securely deleted, destroyed, or anonymised.

Data Breaches

All personal data breaches or suspected breaches must be reported immediately to the Data Protection Lead.

The organisation will:

- Investigate and document all breaches
- Assess the risk to individuals
- Notify the ICO within 72 hours where required
- Notify affected individuals where there is a high risk to their rights and freedoms
- Take corrective action to minimise future risks

A breach register will be maintained.

CCTV, Photography, and Video Recording

CCTV may be used for safety, safeguarding, and crime prevention purposes.

Where CCTV is in operation:

- Appropriate signage will be displayed
- Recordings will be stored securely
- Access will be restricted to authorised personnel
- Footage will only be retained as long as necessary



YOUNG LEWISHAM PROJECT

Photographs and video recordings of children and young people will only be used with appropriate consent and in line with safeguarding procedures.

Training and Awareness

All staff and volunteers will receive appropriate data protection training, including:

- Induction training
- Refresher training
- Breach reporting procedures
- Information security awareness

Compliance with this policy will be monitored regularly.

Monitoring and Review

This policy will be reviewed every two years or sooner if:

- Legislation changes
- ICO guidance changes
- Significant organisational changes occur
- A serious data protection incident takes place

Complaints

Anyone who is dissatisfied with how their personal data has been handled may raise a complaint with The Young Lewisham Project.

If concerns cannot be resolved internally, complaints may be made to:

Information Commissioner's Office

You can find further information at [ICO Official Website](https://ico.org.uk/)



**YOUNG
LEWISHAM
PROJECT**

Linked Policies

This policy should be read alongside:

- Safeguarding Policy
- Child Protection Policy
- Confidentiality Policy
- E-Safety / Online Safety Policy
- Records Retention Policy
- Staff Code of Conduct
- Whistleblowing Policy
- IT Acceptable Use Policy