Manchester Young Lives

Data Protection Policy

Policy Reviewed	April 2021
Reviewed by	Central Office
Review Date	April 2023

CONTENTS

1. AIM

Our organisation aims to ensure that all personal data collected about staff, volunteers, children & young people, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION & GUIDANCE

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's:

	• Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. DATA CONTROLLER

Manchester Young Lives [MYL] processes personal data relating to staff, volunteers, children & young people, parents, trustees, and others, and therefore is a data controller.

MYL is registered as a data controller registered with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES & RESPONSIBILITIES

This policy applies to **all MYL staff and volunteers**, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustees

The board of trustees has overall responsibility for ensuring that our organisation complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

Due to the nature of MYL's processing activities, the organisation is not required to appoint a DPO. The CEO will therefore be responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The Business Support Team is the first point of contact for individuals whose data the organisation processes, and for the ICO.

The Business Support Team are contactable via the following methods:

- **In writing**: Business Support Co-ordinator, Manchester Young Lives, The Addy Young People's Centre, Woodhouse Lane, Wythenshawe, Manchester, M22 9TF.
- **Via email**: info@manchesteryounglives.org.uk
- **Via telephone**: 0161 437 5923

5.3 Chief Executive Officer

The CEO acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for :

- Collecting, storing and processing any personal data in accordance with this policy
- Informing MYL of any changes to their personal data, such as a change of address
- Contacting the Business Support Team in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - To verify any contracts or sharing agreements for personal data with third parties

6. DATA PROTECTION PRINICPLES

The GDPR is based on data protection principles that our organisation must comply with and this policy sets out how MYL aims to comply with these principles.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the organisation can **fulfil a contract** with the individual, or the individual has asked the organisation to take specific steps before entering into a contract
- The data needs to be processed so that the organisation can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed for the **legitimate interests** of the organisation or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a child or young person) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the MYL's record retention schedule

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or young person, or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and children/young people – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Where necessary, establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children, young people or staff and volunteers

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. SUBJECT ACCRSS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject access requests

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the organisation holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email fax to the Deputy CEO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the Deputy CEO

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children attending MYL may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Children and young people aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children and young people at MYL may not be granted without the express permission of the child/young personl. This is not a rule and an individual's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the

individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Deputy CEO. If staff receive such a request, they must immediately forward it to the Deputy CEO.

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations at MYL sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Deputy CEO.

12. PHOTOGRAPHS & VIDEOS

As part of our activities, we may take photographs and record images of individuals within our settings

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photographs and/or video will be used to both the parent/carer and child.

We will obtain written consent from parents/carers, or young people aged 13 and over, for photographs and videos to be taken of young people for communication, marketing and promotional materials.

Uses may include:

- Within centres on notice boards and in brochures, newsletters, etc.
- Outside of MYL by external agencies such as the funders, strategic partners, newspapers, campaigns
- Online on our website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

13. DATA PROTECTION BY DESIGN & DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training and briefing members of staff and volunteers on data protection law, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including :
    - For the benefit of data subjects, making available the contact details of the CEO/Deputy CEO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. DATA STORAGE AND SECURITY OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks, in shared offices, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out with the Centre or Project Manager/Deputy
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff and young people are reminded to change their passwords at regular intervals
- Staff, volunteers, young people or trustees must not store personal information on their personal devices . All personal data must only be stored on the secure remote desktop storage (Skyline)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

See also MYL Information Security Policy

15. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the MYL's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. PERSONAL DATA BREACHES & REPORTING

MYL will make all reasonable endeavours to ensure that there are no personal data breaches.

a) What Is A Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored, or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an email or SMS to the wrong recipient).
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing, and other "blagging" attacks where information is obtained by deceiving whoever holds it.

b) When does It need to be reported?

MYL must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination.
- potential or actual financial loss.
- potential or actual loss of confidentiality.
- risk to physical safety or reputation.

- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

Staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, the Business Support Manager or the Deputy CEO

Once reported to the Business Manager or Deputy CEO, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The CEO or Deputy CEO will acknowledge receipt of the data breach notification and take appropriate steps to deal with the report.

c) Managing and recording the breach

On being notified of a suspected personal data breach, the CEO will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to: -

- Where possible, contain the data breach
- As far as possible, recover, rectify, or delete the data that has been lost, damaged or disclosed
- Assess and record the breach in MYL's data breach register
- Notify the ICO
- Notify data subjects affected by the breach
- Notify other appropriate parties to the breach.
- Take steps to prevent future breaches.

d) Notifying the ICO

The CEO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If it is unclear of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

e) Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, The CEO will notify the affected individuals without undue delay including the contact details of the ICO, the likely consequences of the data breach and the measures MYL have (or intend) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, The CEO will co-operate with and seek guidance from the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then MYL will consider alternative means to make those affected aware (for example by making a statement on MYL's website).

f) Notifying other authorities

MYL will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers.
- Parents.
- Third parties (for example when they are also affected by the breach);
- Local authority.
- The police (for example if the breach involved theft of equipment or data).
- This list is non-exhaustive.

g) Assessing the breach

Once initial reporting procedures have been carried out, MYL will carry out all necessary investigations into the breach.

We will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction, or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, MYL will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is
- The volume of data affected
- Who is affected by the breach (i.e. the categories and number of people involved)?
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation)?
- What has happened to the data?
- What could the data tell a third party about the data subject
- What are the likely consequences of the personal data breach on MYL and any other wider consequences which may be applicable?

h) Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this,we will: -

- Establish what security measures were in place when the breach occurred.
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again.
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice.
- Consider whether it's necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken
- To update the data breach register
- To debrief governors/management following the investigation.

i) Reporting Data Protection concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the CEO/Deputy CEO. This can help capture risks as they emerge, protect MYL from data breaches and keep our processes up to date and effective.

17. TRAINING & MONITORING ARRANGEMENTS

All staff and trustees are provided with data protection briefing as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the MYL's processes make it necessary.

The CEO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full board of Trustees