Cornerstone Building Sulyard Street, Lancaster, LA1 1PX
www.lancashireyouthchallenge.co.uk
Registered Charity: 1163469

Data Protection and Data security Policy

Effective Date: **September 2021**

Trustee Review Date: **September 2023**

1. Statement and purpose

Lancashire Youth Challenge (LYC) store and process the personal data of staff members, freelance staff, volunteers, partners, participants and other individuals for a variety of business purposes.

This policy sets out how LYC will protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires staff members to ensure that the organisation is compliant.

2. Scope

This policy applies to all staff members. Staff members must be familiar with this policy and comply with its terms.

The Chief Executive Office is LYC's Data Controller (DC) and they are responsible for the day-to-day implementation of the policy.

3. GDPR Principles

LYC's staff will comply with the principles of data protection (the Principles) as laid out in the EU General Data Protection Regulations *(GDPR).* These Principles are:

- *Lawful, fair and transparent* – collection of personal data must be fair and LYC must be open and transparent as to how the data will be used.
- *Limited for its purpose* – personal data can only be collected for a specific purpose.
- *Data minimisation* – personal data collected must be necessary and not excessive for its purpose.
- *Accurate* – personal data must be accurate and kept up to date.
- *Retention* – personal data will not be stored longer than necessary.
- *Integrity and confidentiality* – personal data must be kept safe and secure

4. Registration with Information Commissioners Office (ICO)

Having completed the ICO's online 'Registration Self-Assessment' questionnaire it has been established that LYC does not have to register with or pay a data protection fee to the ICO. However, it is important that LYC adheres to the principles of GDPR and understands best practice for managing information

5. Procedures

5.1 – *Lawful basis for processing personal data*

To comply with GDPR, LYC must establish a lawful basis for processing data. Staff members must ensure that any data they are responsible for managing has a lawful basis, agreed by the DC. It is the responsibility of each staff member to check the lawful basis for any personal data they are working with and ensure all of their actions comply with the lawful basis. At least one of the following conditions must apply whenever personal data is processed by a staff member:

- Consent – LYC holds clear, explicit and defined consent for the individual's data to be processed for a specific purpose.
- Contract – the processing is necessary to fulfil or prepare a contract for an individual.
- Legal obligation – LYC has a legal obligation to process the data (e.g. executing a contract)
- Vital interests – processing the data is necessary to protect a person's life or in a medical situation
- Public function – processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- Legitimate interest – the processing is necessary for LYC's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

5.2 – *Deciding which condition to rely on*
Before making an assessment of the lawful basis, staff members must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. It is possible that more than one basis might apply. The basis that best fits the purpose should be noted and not what is easiest.

The following factors should be considered:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same lawful basis the individual would expect?
- What is the impact of the processing on the individual?
- Is the person processing the data in a position of power over the person whose data is being processed?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Is it possible to stop the processing at any time on request, and has stopping the processing been factored in?

The DC will maintain a register of LYC's Personal Data Assets and the lawful basis on which data across the organisation is being processed, and staff members must inform the DC of any new processing. Staff members must consult with the DC on the lawful basis of any processing activity.

6 Special Categories of Personal Data

This means data about an individual which is more sensitive and requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health and sexual orientation.

LYC does ask individuals to complete equal opportunities monitoring forms which does collect this kind of sensitive information. However, the information is anonymised and kept separate to an individual's contact details and used only for monitoring and reporting purposes. Safeguarding reports are password protected.

7 Photography and Film

Occasionally, LYC take photographs and create films of various activities/events, this means that we will collect and store imagines of individuals.

Staff, volunteers, freelancers and participants in LYC's activities will be asked to sign a form that seeks consent for taking, storing, processing and sharing images. Individuals are not obliged to give their consent.

LYC will never release an individual's contact details to outside organisations LYC for their marketing purposes, but may share images for which we have gained consent to use in this way.

8 Responsibilities

8.1 - Staff Member Responsibilities

- Fully understand your data protection obligations.
- Check that any data processing activities you are dealing with comply with this policy and are justified.
- Do not use data in any unlawful way.
- Do not store data incorrectly, be careless with it or otherwise cause LYC breach data protection laws and our policies through your actions.
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.
- Inform the DC of data processing activity so it can be added to the register of LYC Personal Data Assets.

8.2 - The Data Controller's Responsibilities

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Providing data protection advice and training to staff and those included in this policy, including during staff induction.
- Answering questions on data protection from staff members, Board members and other stakeholders.
- Managing subject access requests and responding to individuals who wish to know what data is being held on them by LYC.
- Verifying the lawful basis for processing data and the adequacy of privacy notices.
- Compiling and maintaining an up to date register of LYC Personal Data Assets and the associated lawful basis for processing.

9 Accuracy and Relevance

LYC will ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. LYC will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

10 Data Security

Staff members must keep personal data secure against loss or misuse.

11 Storing Data Securely

- When data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly. LYC uses a password management document to store passwords. Staff members should liaise with the DC on access to this.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The DC must approve any cloud services used to store data.
- Data should be regularly backed up.
- Special attention must be paid to the use of mobile devices and their security – e.g. laptops, tablets or smartphones. Ensure they have strong password protection and up to date anti-virus software.

12 Data Retention

Personal data must be retained for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with the data retention guidelines.

13. Transferring Data Internationally

There are restrictions on international transfers of personal data. Personal data must not be transmitted anywhere outside the UK without first consulting the DC.

14. Rights of Individuals

Individuals have rights to their data which must be respected and complied with in accordance with the guidance set out by the ICO.

LYC will ensure individuals can exercise their rights in the following ways:

14.1 Right to be informed

- Providing a privacy notice, which is concise, transparent, intelligible and easily accessible, free of charge, that is written in clear and plain language.
- Keeping a record of how personal data is used to demonstrate compliance with the need for accountability and transparency.

14.2 Right of access

- Enabling individuals to access their personal data.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

14.3 Right to rectification

- LYC will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay and no later than one month. This can be extended to two months with permission from the DC.

14.4 Right to erasure

- An individual's data must be erased if requested and there is no compelling reason for its continued processing.

14.5 Right to restrict processing

- LYC shall comply with any request to restrict, block or otherwise suppress the processing of personal data.
- LYC is permitted to store personal data if it has been restricted but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

14.6 Right to data portability

- LYC shall provide individuals with their personal data so that they can reuse it for their own purposes or across different services.
- LYC shall provide it in a commonly used, machine-readable format, and send it directly to another data controller if requested.

14.7 Right to object

- LYC shall respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- LYC shall respect the right of an individual to object to direct marketing.
- LYC shall respect the right of an individual to object to processing their data for research and statistics.

15. Privacy Notice

LYC's privacy notice must be supplied or available at the time the data is obtained from the individual. If the data has not been obtained directly from the individual, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged then the privacy notice must be supplied prior to the data being disclosed.

16. Subject Access Requests

16.1 What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, and have access to their personal data.

16.2 How does LYC manage subject access requests?

All requests received by staff members related to subject access requests should be forwarded immediately to the DC for consideration and action in accordance with this policy.

The DC must provide an individual with a copy of the information they request, free of charge. This must occur without delay, and within one month of receipt. LYC endeavours to provide individuals access to their information in commonly used electronic formats. If complying with the request is complex or numerous, the deadline can be extended to two months but the individual must be informed within one month.

Once a subject access request has been made, a staff member must not change or amend any of the data that has been requested. Doing so is a serious criminal offence.

The DC will ensure that all subject access requests are handled in accordance with the guideline set out by the ICO.

16.3 Data portability requests

The DC must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. The DC must provide this data either to the individual who has requested it, or to the data controller they have requested it to be sent to. This must be done free of charge and without delay, and no later than one month.

16.4 Right to erasure

16.4.1 What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed.
- Where consent is withdrawn.
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed or otherwise breached data protection laws.
- To comply with a legal obligation.
- The processing relates to a child.

16.4.2 How LYC deals with the right to erasure

All requests received by staff members related to the right to erasure should be forwarded immediately to the DC for consideration and action in accordance with this policy.

LYC can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

16.5 The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. LYC must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

17. Training, Monitoring, Reporting and Failure to Comply

17.1 Training

All staff members will receive training on this policy as part of their Induction training. The DC will undertake refresher training every two years and will discuss any changes to legislation or policy during staff supervision.

17.2 Reporting breaches

All staff members have an obligation to report actual or potential data protection compliance failures. This allows LYC to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures

Staff members should inform the DC of all actual or potential data protection compliance failures as soon as practically possible, i.e. as soon as they are aware of a breach.

17.3 Monitoring

All staff members must comply with this policy. The DC has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

17.4 Consequences of failing to comply

LYC takes compliance with this policy very seriously. Failure to comply puts both staff members and LYC at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If a staff member has any questions or concerns about anything in this policy, they should contact the DC.