Data Protection Policy

Introduction

At Livewire youth project we may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we work. To that end we will treat personal information lawfully and correctly in accordance with the principles of the General Data Protection Regulation (GDPR) which we fully endorse and adhere to.

This policy applies to the personal data of job applicants, existing and former employees, volunteers including management committee members and trustees, placement students, and members. These are referred to in this policy as relevant individuals.

Definitions

Personal data is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification/membership number, location, online identifier. It can also include pseudonymised data.

Special categories of personal data may include information relating to an individual's health.

Criminal offence data is data which relates to an individual's criminal convictions and offences

Data processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Principles

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) Processing will be fair, lawful and transparent
b) Data be collected for specific, explicit and legitimate purposes
c) Data collection will be adequate, relevant and limited to what is necessary for the purposes of processing
d) Data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) Data is not kept for longer than is necessary for its given purpose
f) Data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures

Types of Data held

We keep several categories of personal data on relevant individuals, we keep this data on file. Specifically, we hold the following types of data:

On staff:

1. Personal information including name, date of birth, address, bank details, telephone number and email address
2. CV's and other information gathered during recruitment
3. DBS clearance number and any criminal convictions (risk assessment associated with where necessary)
4. References from previous employers
5. Tax codes
6. Contract of employment, Job title, Job description and pay grades
7. Internal performance information
8. Training details and copies of certificates

On members:

1. Personal information including Name. Address. Emergency contact telephone number and date of birth
2. Accreditation paperwork and copies of certificates gained through accreditation schemes
3. Medical information

On Counselling Clients:

1. Personal information including Name, Address, Telephone number or email address or that of next of kin and the clients date of birth.
2. Medical information, including doctors and any medication/diagnosis and any illegal drugs or substance misuse.
3. Who lives with the client.

Relevant individual's rights

You have the following rights in relation to the personal data we hold on you:

a) The right to be informed about the data we hold on you and what we do with it
b) The right to access to the data we hold on you. More information on this can be found in the section headed *access to data* in this policy.
c) The right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as *rectification.*
d) The right to have data deleted in certain circumstances. This is known as *erasure.*
e) The right to restrict the processing of the data.
f) The right to transfer the data we hold on you to another party. This is known as *portability.*
g) The right to object to the inclusion of any information.
h) The right to regulate any automated decision-making and profiling of personal data.

Responsibilities

In order to protect the personal data of relevant individuals, those within Livewire who must process data as part of their role have been made aware of policies on data protection.
We also have employees with responsibility for reviewing and auditing our data protection systems.

Lawful Basis of Processing

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.
Where no other lawful basis applies, we may seek to rely on the relevant individual's or parent/guardian where appropriates consent.
At Livewire the lawful basis for keeping data on employees, volunteers, placement students, management committee members and trustees is *CONTRACT* the processing is necessary for a

contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
The lawful basis for keeping data on members, where consent is not necessary for example membership forms is *LEGITIMATE INTEREST,* the processing is necessary for our legitimate interests in the individual.

Access to Data
As stated above relevant individuals have a right to access the personal data that we hold on them. To exercise this right, individuals should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the relevant individual making the request. In these circumstances, a reasonable charge will be applied.

Data Disclosures
Livewire may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a) Any employee benefits operated by third parties.
b) Disabled individuals – whether any reasonable adjustments are required to assist them at work.
c) Individuals health data – to comply with health and safety or occupational health obligations towards the employee.
d) For statutory Sick pay purposes.
e) The smooth operation of any employee insurance policies or pension plans.
f) To assist law enforcement or a relevant authority to prevent or detect crime or prosecute offences or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security
All employees are aware that hard copy of personal information should be kept in a locked filing cabinet or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files of written information of a confidential nature in a secure manner so that they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all laptops etc when attended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on a removable storage media that media must itself be kept in the safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to relevant individuals should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) Ensuring that data is recorded on such devices only where absolutely necessary.
b) Using an encrypted system – a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) Ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow Livewire's rules on data security may be dealt with through our disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of failure.

Requirement to notify breaches

All data breaches will be recorded on our Data Breach Register. Where legally required we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees will receive training where necessary which covers basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller for Livewire is appropriately trained in their role under the GDPR.

Records

Livewire keeps records of its processing activities including the purpose for the processing and retention periods in its Data Record. These records will be kept up to date so that they reflect current processing activities.

Review

This policy will be reviewed annually unless changes in law necessitate an earlier review. The next review of this policy is due on 14/09/2023

Issue 6	Date: 14/09/2022