Data Protection Policy

Introduction

LIFE-FORCE Centre (the Organisation) processes Personal Data which is held in regulated formats and as such are required to have a General Data Protection Regulation (GDPR) Policy that is implemented with due care and attention and to a high standard. The EU GDPR regulations come into effect on the 25th May 2018 and are enforced by the Information Commission's Office (ICO). This new legislation legally requires the Organisation to take responsibility for all the Personal Data it collects and processes and as such to have appropriate policies and procedures in place that ensure each individual's right to have a workplace culture of data privacy and security is provided.

The Information Commissioners Office

The ICO is a UK independent authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals. The ICO upholds these areas by ensuring organisations abide by and comply with the following legislation.

- Data Protection Act (DPA) 1998
- Electronic Identification and Trust Services for Electronic Transactions Regulations (eIDAS) 2016
- Environmental Information Regulations 2004
- Freedom of Information Act (FOI) 2000 & 2004
- General Data Protection Regulations (GDPR) 2018
- INSPIRE Regulations 2009
- Privacy and Electronic Communications Regulations (PECR) 2004, 2011, 2015 & 2016
- The Re-Use of Public Sector Information Regulations 2015

Organisational Responsibilities

LIFE-FORCE is a registered member with the ICO and the Controller for the Organisation is the Director. The Controller determines the purpose and how any Personal Data is processed and has the responsibility to establish practices and policies for the Organisation. The Organisation's Members include Employed and Self-Employed Staff; Tutors; Team Counsellors; Diploma/Degree Counselling Students. The Organisation has a duty of care to protect its Members', Students' and Clients' Personal Data, by being transparent and accountable, when carrying out direct marketing; requesting access to their personal data; processing, storing, maintaining, retaining and destroying their information safely and securely.

The Organisation's office has a security key code lock entrance which is restricted to authorised staff only who also lock the office with a key before leaving the premises. All visitors to the office are always accompanied by a member of staff.

Breaches in Data Protection

All potential or actual breaches of data **must** be reported to the Organisation's Director immediately, in person or by telephone. The Organisation has a duty to report any serious breach of data to the ICO and to also notify its Members and Clients individually of any serious breach of data. This applies to actual or potential data protection breaches of security which could lead to accidental or unlawful:

- Destruction of data
- Loss of data in paper or electronic format
- Alteration of personal data without permission
- Communication of the wrong information to an unintended recipient
- Members including clients having unauthorised access to data
- Passing personal/sensitive data to a third party without the Data Subject's consent
- Not having the right level of security in place when transmitting/transporting data thereby risking interception.

Members Responsibilities

All Members are required to adhere to the DPA 1998; GDPR 2018 and the Organisation's GDPR Policy. It is essential they respect the privacy rights of other Members and Clients. Members are required to minimise any risk to the Organisation of being exposed to a fine and/or damage to its reputation due to processing any Personal Data incorrectly in accordance with the law and this policy. In such circumstances that this occurs the ICO can take action to change the behaviour of the Organisation and any individuals that collect, use and keep personal information. This includes criminal prosecution, non-criminal enforcement and auditing. The ICO has the power to impose a civil monetary penalty on a data controller of up to £500,000. Criminal prosecutions under Section 55 of the Data Protection Act can attract an unlimited fine.

Members are Data Processors and will be required to sign the Organisation's Non-Disclosure Agreement accordingly.

Data Protection Criteria

Personal Data

Personal Data relates to a living individual (a Data Subject), who can be identified by any of the following data parameters.

a) General or factual information e.g. Name, address, date of birth.
b) Or it can be by an opinion about the Data Subject, e.g. Performance appraisal.

Sensitive Personal Data

Sensitive Personal Data is referred to in the GDPR as 'Special Categories of Personal Data', which are broadly the same as those in the DPA 1998 and includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings and specifically now includes the processing of genetic, biometric data and the use of pseudonyms. Sensitive Personal Data can only be processed under strict conditions, and requires the explicit consent of the person concerned.

Types of Formats

Personal Data which is held in any of the following formats is subject to data protection.

a) Electronically in an automated system e.g. on a computer, database, text message, e-mails.
b) Paper documents which comprise part of a relevant filing system e.g. forms, letters.
c) An accessible record not part of an automated system or relevant filing system, including health, educational and verbal records.

Consent

The Organisation is required to have the appropriate processes and procedures in place to ensure it obtains consent from Members, Clients, and Students (Data Subjects) before processing their data. The following points must therefore be adhered to by both the Organisation and its Members:

- Consent must be a positive indication and cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent can only be accepted where it is freely given, specific, informed and is an unambiguous indication of the individual's wishes.
- Where consent is given a record must be kept documenting how and when it was given.
- Ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR.
- Consent can be withdrawn by the individual at any time.

Subject Access Request (SAR)

The GDPR consider personal privacy a top priority and that Members and Clients have the right to be informed about how their Personal Data is stored, accessed, used, updated and deleted. The DPA states all Data Subjects /Members and Clients of the Organisation have a legal right to ask to see any Personal Data related to themselves which is held by the Organisation, and that the Organisation is legally obliged to meet any such Subject Access Request (SAR). A Subject can put a request in writing to the Organisation's Director for copies of their Personal Data relevant to the individual and the Organisation is legally obliged to provide this information for no fee within 30 days.

If a Member receives a request from one of their Clients or any Third Party they need to inform the Organisation's Director or representative of a SAR immediately upon receipt. They must also inform the Director of all disclosure requests from law enforcement authorities or other third parties whose identity must be verified by the appropriate ID relevant to their place of employment. The office staff must ensure the Data Subject signs the relevant Organisation's Consent to Disclose Form(s) for Counselling Service Information Form and/or Case Notes, before providing copies of confidential client records and Personal Sensitive Data. They should also make sure the requester signs a Confirmation of Receipt form and the type of ID presented is recorded on the form along with any reference number. The Organisation should not retain copies of counsellor client case notes. The Organisation maintains an audit trail of SARs and formal complaints in the form of a SAR Disclosure Record Sheet which details the dates of the initial request, the acknowledgement and provision of requested information.

Data Protection Act Principles

In accordance with the requirements outlined in the GDPR, the Organisation must process each Member's/Client's Personal Data using the 8 regulated principles of the DPA 1998 which state that this data must be:

1. **Processed lawfully, fairly and in a transparent manner in relation to individuals**.
2. **Processed for one or more specified and lawful purpose.**
3. **Adequate, relevant and not excessive for the purpose.**
4. **Accurate and kept up to date.**
5. **Not kept for longer than necessary for the purpose.**
6. **Processed in line with the Data Subject's rights**
7. **Kept secure.**
8. **Not transferred to people or organisations situated in other countries without adequate protection.**

Standards and Criteria for the Regulated Principles

If the Organisation or any of its Members fail to comply with these principles they can be fined for breach of legal requirements by the ICO. Therefore all Members must adhere to the following standards and criteria in relation to these principles.

1st Principle – Processed lawfully, fairly and in a transparent manner in relation to individuals
Fairly processed requires the Organisation and Members to:

a) Be transparent, clear and open with Clients and tell them how the Personal Data collected from them will be used e.g. To arrange counselling sessions, to assess performance.
b) Handle Personal Data how they would expect and not to use this information in a way that unjustifiably would have a negative effect on the individual.

Lawfully processed requires the Organisation and Members to:

a) Gain consent by using an appropriate data protection statement before collecting Personal Data.
b) To be aware that Sensitive Personal Data requires explicit consent from the individual.
c) Obtain Parental or guardian consent for CYP under 18 years old and ensure the referring parent or guardian gives verbal confirmation that they will inform the other parent or guardian. Young

people aged 16-18 years old if considered Guillick Competent and self-referring can give verbal consent themselves.

d) Ensure indirect Personal and Sensitive Data that is provided by a third party has the client's consent for their information to be shared.
e) Offer clients the opportunity 'to be forgotten' by removing their Personal Data e.g. cross shredding information, unsubscribe to further communication in an easy and transparent way or use an unsubscribe statement at the bottom of emails.

2nd Principle – Personal Information must be Processed for a Legitimate Purpose

This principle requires the Organisation and Members to:

a) Be clear and transparent to the individual about why they are collecting the data i.e. for a specified, explicit and legitimate purpose.
b) Not use it for any other purpose e.g. solely for the purpose of providing counselling sessions.

3rd Principle – Personal Information must be Adequate, Relevant and not Excessive for the Purpose

This principle requires the Organisation and Members to:

a) Collect adequate, relevant and limited Personal Data to what is necessary in relation to the purpose of the information is needed for the specific task.
b) When collecting Sensitive and Personal Data, to only collect the absolute minimum required.

4th Principle – Personal Information Must be Accurate and Up to Date

This principle requires the Organisation and Members to:

a) Ensure they check the quality and accuracy of the Data before using it.
b) Ensure inaccurate data is erased or rectified without delay and notify the Organisation, other Members or third parties where appropriate.
c) Always record the source of the Data and to evidence how and when the Data Subject gave consent for their Personal Data to be used.

5th Principle – Personal Information Should Not kept for Longer than is Necessary

This principle requires the Organisation and Members to:

a) Be responsible for not keeping Data for longer than needed.
b) Ensure all destruction is carried out securely by shredding or confidential waste collection.
c) Adhere to the stipulated retention periods as detailed below.

6th Principle – Personal Information Must be Processed in Line with the Data Subject's Rights

This principle requires the Organisation and Members to:

a) Be aware that Members, Clients and Students (Data Subjects) have the right to request access to copies of any Personal or Sensitive Data that the Organisation holds in any types of format.
b) Subjects have a right to object to processing that is likely to cause or is causing them damage or distress.
c) Ensure they have consent from Data Subjects to use their data for direct marketing. The Data Subjects have the right to withdraw their consent at any time to prevent the processing of their data for direct marketing.
d) Be aware the Organisation is lawfully required to obtain consent for processing data. The Data Subject has the right to object to a decision being taken by automated means.
e) Understand the Data Subject has the right to have any inaccuracy of personal data rectified, blocked, erased or destroyed.
f) Understand the Data The Organisation maintains an audit trail of SAR and formal complaints in the form of a Disclosure Record which details the dates of the initial request, the acknowledgement and provision of requested information
g) Subject has the right to claim compensation for damages caused by a breach of the Data Protection Act and GDPR Regulations.

7th Principle – Personal Information Must be Kept Secure

This principle requires the Organisation and Members to:

a) Ensure all Data is securely held and stored from the point of collection to destruction, with access to the information being strictly prohibited to necessity only.
b) To lock computers when not in use and to keep the password private. Also, to make sure electronic data based and spread sheets of Data are password protected.
c) Securely store, transport and lock up paper copies of documents containing Personal Data, Sensitive Data or Organisational sensitive information when not in use over night/weekend.
d) Ensure all emails have a confidentiality signatory which asks a non-intended recipient to delete the content and attachments of any incorrectly sent emails and also states the contents must not be copied shared or disclosed without permission of the Organisation/Member.
e) Be aware the mobilisation and/or transference of personal and sensitive data under GDPR needs to be encrypted. Therefore, the mobilisation and/or transference of data via e-mail that contains personal and sensitive data should be sent using an encrypted e-mail or if considered necessary as an attached document that has been password protected. Members should also ensure they use a secure/encrypted email service provider who meets the GDPR regarding the safe transmission and storage of information.
f) Immediately report all breaches of security incidents and accidental sharing of Data to the Director.
g) Ensure you have explicit consent from your Data Subject before share information with third parties.

8th Principle – Personal Information Must not be Transferred to Other Countries without Adequate Protection

This principle requires the Organisation and Members to:

a) Not to enter into arrangement which involves transferring Personal or Sensitive Data outside the European Economic Area (EEA).
b) Not to knowingly correspond electronically outside the UK by email/text messages with Clients or each other.

Additional Requirements

The Organisation and Members are also required to:

a) Anonymise Data where ever possible and use a client code on invoices to third parties and client initials in paper/electronic communication with the Office.
b) Not share data with any third party for marketing, and only share information with trusted third parties when the Data Subject has given verbal/written consent.
c) Ensure for counselling referrals from third parties that each individual client has given their consent for their Personal Data to be shared and their explicit consent for their Sensitive Data to be shared with the Organisation.
d) Maintain an opt in/opt out marketing e-mail mailing list so that individuals will not be sent information unless they have already provided their explicit written consent.
e) Ensure extra care is taken when sending bulk emails to multiple recipients to ensure their contact details remain unknown to each other by copying them in 'blind' (BB).