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 Data Protection Policy that is implemented with due care and attention and to a high standard. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which is enforced by the Information Commissioner's Office (ICO). This 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 Commissioner's Office

The ICO is a UK independent public 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) 2018
- General Data Protection Regulation (GDPR) 2018
- Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations (PECR) 2003
- Freedom of Information Act (FOI) 2000

Organisational Responsibilities

LIFE-FORCE Centre is a registered member with the ICO and the **Centre Director** is the **Controller** for the Organisation. The Controller determines the purpose of any personal data and how this is processed and has the responsibility to establish practices and policies for the Organisation.
The Organisation's **Members** include; management; employed and self-employed staff; tutors; team counsellors; diploma/degree counselling students on placement and third-party contractors.
The Organisation has a duty of care to protect its Members' and Clients' personal data, by being transparent and accountable when undertaking the following activities:

- **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.

Members Responsibilities

All **Members** are **Data Processors** and as such are required to adhere to the DPA 2018; GDPR 2018 and the Organisation's Data Protection 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.
As all Members are Data Processors, they are required to sign a **LIFE-FORCE Non-Disclosure Agreement**.

Data Protection Criteria

Personal Data

Personal data relates to an 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) An opinion about the Data Subject, e.g. Performance appraisal.

Special Categories of Personal Data

Certain types of personal data are sensitive and therefore need additional protection under the GDPR. These are referred to as 'special categories of personal data' and refer to the use of personal data **revealing** or **concerning** a person's:

- **Racial or ethnic origin**
- **Political opinions**
- **Religious or philosophical beliefs**
- **Trade union membership**
- **Genetic data**
- **Biometric data**
- **Physical or mental health**
- **Sexual life or sexual orientation**

The processing of a Data Subject's special categories information is prohibited except under limited circumstances. As such sensitive personal data regarding any of these categories, and in particular mental health in relation to the provision of counselling services, only be processed under strict conditions one of which requires the **explicit** consent of the person concerned.
(Ref. GDPR, Article 9, pt (a))

The above special categories do not include personal data about criminal allegations, proceedings or convictions, as separate rules apply to criminal offences.

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 Requirements

The Organisation has the appropriate processes and procedures in place to ensure it obtains consent from Members and Clients (**Data Subjects**) before processing their data.
As such the following **consent requirements** must 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 when it is freely given, specific, informed and is an unambiguous indication of the individual's wishes.
- Written consent or verbal consent given by clients during remote counselling must be recorded and kept on a document detailing how and when it was given.
- Consent mechanisms must 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 must be reviewed to ensure it meets the standards of the GDPR.
- Consent can be withdrawn by the individual at any time.

Principles of Data Protection

The **7 principles of GDPR** are an important part of data protection law which form the foundation for best practices when processing personal data. The Organisation aims to adhere to and implement these key principles throughout all our data management procedures when processing Members' and Clients' personal data, these are detailed below.

The 7 Principles of GDPR

1. **Lawfulness, fairness & transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity & confidentiality**
7. **Accountability**

Criteria for the 7 Principles of GDPR

If the Organisation or any of its Members fail to comply with these 7 principles, they can be fined for breach of legal requirements by the ICO. Therefore, all Members must adhere to the following criteria in relation to these principles.

1st Principle – Processed **lawfully**, **fairly** and in a **transparent** manner in relation to individuals

Lawfully processed requires the Organisation and Members to:

a) Gain written or verbal 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 Member's or Client's consent for their information to be shared.
e) Offer Members and Clients the opportunity 'to be forgotten', unless there is a legal exception to maintain records, 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.

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 progress.
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.

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 electronic deletion, shredding or confidential waste collection.
c) Adhere to the stipulated Organisation's retention periods as detailed below.

6th Principle – Personal Information Must be Kept **Secure** and **Protected** against Unlawful or Unauthorised processing, access, loss, destruction or damage**.**
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 electronic 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 standards regarding the safe transmission and storage of information.
f) Immediately report all breaches of security incidents/accidental sharing of data to Centre Director.
g) Ensure they have explicit consent from their Data Subject before sharing information with third parties.

7th 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 other Members or Clients.

Privacy Management Criteria

Personal Information Must be Processed in Line with the Data Subject's Rights
These criteria require the Organisation and Members to:
a) Be aware that Data Subjects (Members and Clients) have the right to request access to copies of any personal or sensitive data that the Organisation holds in any types of format.
b) Be aware Data 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 Organisation maintains an audit trail of a SAR in form of a **SAR Disclosure Record** which details the dates of the initial request, the acknowledgement and provision of requested information.
g) Understand the Organisation maintains an audit trail of concerns or formal complaints in the form of a Concerns/Complaint Record which details the dates of the initial receipt, the acknowledgement, the process and outcome.
h) Be aware the Data Subject has the right to claim compensation for damages caused by a breach of the Data Protection Act 2018 and GDPR Regulations.

Additional Privacy Management Criteria

These additional criteria require the Organisation and Members to:

a) Ensure the sharing of personal information is strictly on a need to know basis and as such is kept to an absolute minimum at all times.
b) Anonymise data wherever possible and use a client code on invoices to third parties.
c) Minimise the use of clients' names and only use their initials, or if necessary use first name and initial of surname, when communicating with the Office by paper or electronically regarding service arrangements.
d) Not share data with any third party for marketing, and only share information with trusted third parties when the Data Subject has given explicit verbal/written consent.
e) 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.
f) Whenever possible and applicable to always seek to gain written consent, as opposed to verbal consent, from another Member or Client. When Members are providing remote counselling, and written consent is not practically possible, then verbal consent must be gained instead and recorded by the Member on the relevant document in the client's consent statement section as **'Informed Verbal Consent Obtained'** and the **date**.
g) 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.
h) 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' (Bcc).

Subject Access Request (SAR)

The GDPR considers 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 Data 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 Centre Director or representative for a SAR immediately upon receipt. They must also inform the Centre Director of all disclosure requests from law enforcement authorities or other third parties parties. If available, the requesting person's identity ID relevant to their place of employment must be recorded. The office staff must ensure the Data Subject signs the relevant LIFE-FORCE **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 in the form of a **SAR Disclosure Record Sheet** which details the dates of the initial request, the acknowledgement and provision of requested information.

Breaches in Data Protection

All potential or actual breaches of data **must** be treated as strictly private and confidential and reported to the Organisation's Centre Director immediately by email. The Organisation has a duty to assess the situation and report any serious breach of data to the ICO and to also notify its Members and Clients individually of any serious breach of data that relates to themselves. This applies to all potential or actual serious data protection breaches of security which could lead to accidental or unlawful:

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

Timeline Statement

The Member is then required to write a **Timeline Statement** regarding the breach of personal data and email this confidentially the Centre Director. The statement must include the following information:

a) Date and nature of original personal data collected, where and how retained by Member
b) Initials of person whose personal data has been lost
c) Nature of professional relationship with Member
d) Name and description of mislaid or lost personal data
e) Date, time, place of incident
f) Description of the incident and efforts made to recover the personal data
g) If applicable, date discussed with supervisor and outcome of this meeting
h) Whether or not the Member is still in contact with the person concerned
i) Date of any action taken
j) Description of any changes made by the Member regarding their data protection procedures
k) Signed by Member and dated

Summary Statement

The Centre Director and Service Support Manager review the Timeline Statement and together agreed the contents of a **Summary Statement,** which is added to the document, and details the required course of action the Member must implement. This will include a decision whether or not the breach of personal data is serious and as such if the Course Director needs to inform the ICO. Members who are students on placement are required to provide a copy of the completed Timeline Statement to the Course Director at their training organisation.

LIFE-FORCE Centre Retention Periods

Name of Data	Stored	Retention Period	Disposal
Accounting & Financial Records	Locked Cupboard/ Filing Cabinet	6 Fiscal Years	Double Cross Shredder
Complaint Letters and Responses	Locked Filing Cabinet	7 Years	Double Cross Shredder
Emails	On the Computer	3 Years Maximum	Electronically Deleted
Staff Recruitment and Employment Contracts	Locked Cupboard	6 Years after Leaving	Double Cross Shredder
Review Document Latest Year	Locked Cupboard/ On the Computer	6 Years after Leaving	Double Cross Shredder /Electronically Delete
Declined Staff Application Documents	Locked Filing Cabinet	1 Year Max	Double Cross Shredder
Diary Room Hire Invoices (Electronic)	On the Computer	6 Fiscal Years	Electronically Deleted
Subject Access Request	Locked Filing Cabinet	7 Years	Double Cross Shredder
CPD Training Courses	Locked Cupboard	3 Years after Course	Double Cross Shredder
CPD – Email Address Book	On the Computer	Up until End of Course	Electronically Deleted
Indep Practitioner Reg Docs, Membership & Insurance	On the Computer	6 Months after Non Use of Rooms / Upon Leaving	Electronically Deleted

Counselling Service Retention Periods

Name of Data	Stored	Retention Period	Disposal
Counselling E-mail Enquiries & Forms	On the Computer	6 Months	Electronically Deleted
Client Referral Forms	On the Computer	3 Years	Electronically Deleted
Client Referral Documents	Locked Office/Filing Cabinet	3 Years after Closure	Double Cross Shredder
Client Referral DNA	Locked Cupboard	6 Months after Contacted Service	Double Cross Shredder
Complaint Letters and Response	Locked Filing Cabinet	7 Years	Double Cross Shredder
Counsellor Case Notes	Locked Filing Cabinet	7 Years after Closure	Double Cross Shredder
Counsellor Recruitment Documents & Contracts	On the Computer	6 Years after Leaving	Electronically Delete
Declined Counsellor Application Documents	Locked Filing Cabinet	1 Year Max	Double Cross Shredder
Counsellor CPD Update Documents Latest Year	On the Computer	6 Years after Leaving	Electronically Delete
Counsellor Renewal Certs; Insurance, Membership, ICO, First Aid, & CPD	On the Computer	6 Years after Leaving	Electronically Deleted
Referral Text Messages	On Office Mobile/iPad	6 Months Minimum	Electronically Deleted
Subject Access Request	Locked Filing Cabinet	7 Years	Double Cross Shredder
Student Placemts Reg Docs, Membership & Insurance	On the Computer	6 Years after Leaving	Electronically Deleted

Code of Practice for the Use of Telephones & Mobile Phones

The Organisation has a responsibility and the duty of care to ensure their Staff, Team Counsellors and Diploma/Degree Student Counsellors on Placement (Members) communicate and transfer clients' data in a confidential way within the Counselling Service/Placement Organisation. This Code of Practise provides guidance to Members to ensure that when they communicate and transfer clients' data using, telephones, mobile phones, printers, mobile computers and iPads that this is done in a way that ensures safe procedures.

Contacting Clients

When contacting clients Members should use discretion and establish prior to departing with any personal information that they are speaking to the appropriate person on the phone. If they are unavailable a brief message should be left ensuring the minimum amount of information is communicated within the voice message and that this does not include any Personal or Sensitive Data or the name of the Counselling Service, e.g. "This message is for Christine can you please contact John on 01206-791661".

Office Mobile Phone

The Organisation has a dedicated office mobile phone 07407553582. This phone is protected by a PIN number which is only given to office staff. The phone is used by office staff for contacting clients and sending text messages to Counsellors about client referrals within which only the client's first name and initial of surname can be used and practical appointment details can be specified but further personal client details must not be included. E.g. Appointment required for new client Mary J on Thursdays at 2pm please contact the office. The mobile is switched off when not in use and outside office opening hours.

In order to ensure text messages are sent to the correct counsellor this dedicated mobile phone has the counsellors' phone numbers in the contact list. Counsellors should ensure they take responsibility to inform the office as soon as possible if they change their mobile number.

Counsellors can contact the office using the office mobile number regarding client referral arrangements but no client details should be included in these messages other than the client's initials, or if needed first name and initial of surname, day and time of the appointment.

Counsellors who need to contact the office regarding general enquiries and room booking arrangements should send an email rather than leave a message on the landline answer phone as this is checked on a less frequent basis.

Mobile Phones

Counsellors have a responsibility and duty of care to their clients to protect their data and the best practise regarding this is to password protect the mobile phone used for work from unauthorised access. When charging mobile phones through a USB port on a laptop/iPad, Members have a responsibility to ensure their mobile phone cannot be viewed or accessed without authorisation.

Phone Messages

When listening to answer phone or voice mail messages Members have a responsibility to implement telephone monitoring by being aware of their surroundings and ensuring they listen to their messages within a confidential environment. Good practise is to delete client's phone or voice messages after listening to these or every 3 months.

Text Messages

When sending and receiving text messages from clients, Members need to be responsible and accountable for communicating in a confidential manner in order to ensure no breach of data occurs. The Organisation's best practise recommendation is to have the mobile phone used for work set so that only the sender's details are displayed on the screen and not the actual text message content. When sending text messages these should be as brief as possible, with the content kept to the minimum amount of information as necessary and should NOT include any Personal or Sensitive Data. All text messages should be deleted every 6 months except any received that contain Personal or Sensitive Data which should be deleted straight away.