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 **Data 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' (**'Data Subjects'**) personal data, by being transparent and accountable when undertaking the following activities:

- **administering any accounts**
- **processing bank details for payments**
- **requesting access to their personal data**
- **processing, storing, maintaining, retaining and destroying their information safely and securely.**
- **carrying out direct marketing and marketing research**
- **prevention and detection of fraud**

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 which is not 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 a Member or Client (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, family & lifestyle / social circumstances, financial details, other relevant information.
b) An opinion about the Data Subject, e.g. Performance appraisal.

Processing Personal Data

As such the processing of a Data Subject's personal information is prohibited except under specified lawful bases which are as follows:

- **Consent**
  The Data Subject has given clear consent to process their personal data for a specific purpose.
- **Contractual obligation**
  The processing is necessary for a contract with the individual, or because they have asked the Organisation to take specific steps before entering into a contract.
- **Legal obligation**
  The processing is necessary for the Organisation to comply with the law (not including contractual obligations)**.**
- **Vital interests**
  The processing is necessary to protect someone's life.
- **Public task**
  The processing is necessary to perform a task in the public interest or for the Organisation's official functions, and the task or function has a clear basis in law.
- **Legitimate interests**
  The processing is necessary for the Organisation's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

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**

NB. The above special categories do not include personal data about criminal allegations, proceedings or convictions relevant to a Data Subject, as separate rules apply to criminal offences.
For further information visit ICO website: Criminal Offence Data.

Processing Special Category Data
As such the processing of a Data Subject's special categories information is prohibited except under specified additional conditions which are as follows:

- **Explicit consent by Data Subject**
- **Employment, social security and social protection**
- **Vital interests**
- **Not-for-profit bodies**
- **Made public by the data subject**
- **Legal claims or judicial acts**
- **Reasons of substantial public interest**
- **Health or social care**
- **Public health**
- **Archiving, research and statistics**

This means in order to process personal sensitive data that comes under any of these special categories, in particular mental health in relation to the provision of counselling services, **at least one or more** of the personal data lawful bases **and** one of the special category conditions must be applicable, for example the person concerned has given their **consent** and **explicit consent,** see the definitions below. Therefore, regarding clinical practice, the counsellor should gain each Client's explicit consent to process any of their sensitive personal information by asking them to sign a LIFE-FORCE Counselling Service Client Data Protection Agreement.

Personal Data 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 Criteria

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 criteria** 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.
- Consent is given by a Data Subject at the point when they contact the Organisation by free choice, e.g., by email, website contact form, phone, answerphone message, in writing or in person.
- Explicit consent is given by a Data Subject when the consent is affirmed in a clear statement, this can be verbal or written, eg., by completing the Counselling Enquiry Form Consent Statement, signing a Client Data Protection Agreement or similar means.
- 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 GDPR standards. 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 given does not need to be reviewed, GDPR does not set a specific time limit for consent. If processing operations or purposes evolve, and the original consents are no longer specific or informed enough, the Organisation will seek fresh consent or identify another lawful basis**.**
- Consent can be withdrawn by a Data Subject at any time. The Organisation follows the ICO guidance that states: 'The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. ' This means that there may be times where the processing of personal and special category data, that was collected when consent was provided, will still need to continue.

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 and special categories of 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 and special categories requires explicit consent from the individual.
c) Obtain parental or guardian consent for CYP under 18 years old and depending on the circumstances ensure the referring parent or guardian gives verbal confirmation that they will inform the other parent or guardian and note this on the Child & Young Person Referral Form. Young people aged 13-17 years old, if considered Gillick Competent and self-referring can give verbal consent themselves.
(Ref. Gillick Competence Policy)
d) Offer Members and Clients the opportunity to have their personal data and special categories erased, this is also known as the 'right to be forgotten', by removing their personal data/special categories e.g. cross shredding referral records or case notes records, unsubscribe to further communication in an easy and transparent way or use the unsubscribe statement at the bottom of emails. Certain circumstances may prevent this right being actioned for example there is a legal requirement to maintain records such as for a current police investigation.
(Ref. Case Notes Policy)

Fairly processed requires the Organisation and Members to:

a) Be transparent, clear and open with Clients and tell them how the personal data and special categories data collected from them will be used e.g. to arrange counselling sessions.
b) Handle personal and special categories data securely and not to use this information in a way that unjustifiably would have a negative effect on the individual.

2nd Principle – Personal Information and Special Categories 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 untoward purpose e.g. it is used solely for the purpose of providing counselling sessions.

3rd Principle – Personal & Special Categories 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/special category data to what is necessary in relation to the purpose of the information which 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's other Members or third parties where appropriate. The Organisation aims to update its personal data records straight away following notification of any changes in personal data information.
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 ensure data stored electronically, including external drives e.g. `USB sticks are password protected. To minimise or avoid use of external drives where possible.
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.

Criteria for Data Subject's Rights

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 Subject Access Request (SAR) in form of a **Subject Access Request 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 2 and GDPR Regulations.

Privacy Management Criteria

These privacy management criteria require the Organisation and Members to:

a) Ensure the sharing of personal information both within and outside the Organisation is on a strictly need to know basis and as such is kept to an absolute minimum at all times.
b) Only share personal information with others, such as office staff, counsellors, medical experts, family members, insurers and solicitors, if it is to provide a counselling service &/or if it considered to be for the benefit of the person concerned.
c) Anonymise data wherever possible and use a Client code on invoices to third parties.
d) 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.
e) 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.
f) 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.
g) 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**.
h) Maintain an opt in marketing e-mail mailing list so that individuals will not be sent information unless they have already provided their explicit written consent. When an individual opts out, they are removed from the marketing mailing list and relevant systems.
i) 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) and our marketing e-mails are sent out via MailChimp.

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 & special categories 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/special categories 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 needs to put a request in **writing** to the Organisation's Data Controller for copies of their personal/special categories data and this is usually provided free of charge and within 30 days. The exception being, the Organisation reserves the right to charge a reasonable administration fee and extend the time period by a further 2 months if the request is manifestly unfounded or vexatious and/or very complex.

Client SAR to Office or Counsellor

When the Office or a counsellor receives a SAR from one of their Clients or any third party, including law enforcement authorities, then the relevant procedures as detailed below must be followed. If the client makes a verbal request to the counsellor then they should inform the client to put their request in writing by email/ letter to themselves or to the Office by email. Also, upon receipt of a written SAR the counsellor must inform the Organisation's Data Controller by email straight away.

Client Consent Procedure

A Client SAR can be for counselling service information &/or client case notes. When a written SAR is received from a Client by the Organisation / counsellor then **before** providing copies of confidential Client records and personal sensitive data, the Office emails the Client one or both of the following **Consent to Disclose Forms**, as applicable to the nature of the SAR, for them to complete and sign by hand.

A. Consent to Disclose Form - Counselling Service Information
The Service / counsellor provides a Counselling Service Information Letter detailing information such as frequency of attendance, number of sessions and main theme of the therapeutic work.

B. Consent to Disclose Form - Case Notes
The counsellor provides a copy of the Client's Case Notes.

Section A: Counselling Service Information Procedure

1. Office Receives the SAR

When a written SAR for counselling service information is received by the Organisation then the Office should follow the procedure below.

a) The Office emails the Client a **Consent to Disclose Form - Counselling Service Information** which they are required to fill in, sign by hand and return to the Office. In signing the form, the client themself accepts responsibility to provide any third party requests with the information issued by the Organisation.

b) The Client presents 2 forms of ID, (see **ID Summary Table for Client SAR** below), online or in-person to the Office who records the details on a **Confirmation of Receipt Form**, which is for Office use only. If presented online then the Office signs the Confirmation of Receipt Form on behalf of the client.

c) Within 30 days from receipt of the SAR, the Office provides the Client with a **Counselling Service Information Letter**, either by email as a password protected document, or as hard copy by post or in-person.

d) The Office does not need to provide the counsellor with a copy of the completed Consent to Disclose Form or Counselling Service Information Letter.

e) If applicable, the Client provides a third part request with the Counselling Service Information Letter.

f) The Office fills in and signs by hand the **Consent to Disclose Form: Section B** to record the date and how the letter was provided, and that this procedure has been completed.

g) The Office does not need to complete a **SAR Disclosure Record Sheet**.

h) All the SAR documents including the completed Consent to Disclose Form(s) and Confirmation of Receipt Form are saved on the Office system, the completed hard copies are then shredded, and the electronic versions are saved for 3 years after which they are electronically deleted.

2. Counsellor Receives the SAR

When the request for counselling service information is received by the counsellor, in writing and not the Office, then the counsellor should follow the procedure below. Alternatively, the counsellor can request the Office writes and provides the client with a **Counselling Service Information Letter** instead of them doing this themselves. However, if a student counsellor receives such a request, they should inform the Office who will write the letter.

a) The counsellor should provide the Client with a **Consent to Disclose Form - Counselling Service Information** either by email or as hard copy which the Client is required to fill in, sign by hand and return to the counsellor. In signing the form, the client themselves accepts responsibility to provide any third party requests with the information issued by the Organisation.
b) The counsellor does not need to see the Client's ID.
c) The counsellor then provides the Client with a **Counselling Service Information Letter**, within 30 days from receipt of the SAR.
d) If applicable, the Client provides a third part request with the Counselling Service Information Letter.
e) The counsellor fills in and signs by hand the **Consent to Disclose Form - Counselling Service Information: Section B** to record the date and how the letter was provided, and that this procedure has been completed.
f) The counsellor returns the completed form to the Office who provides them with a copy for filing with their client records.
g) The counsellor either saves the form and letter electronically or in hard copy for 7 years after closure of contract following which both documents should be deleted/shredded.

Section B: Case Notes Procedure

1. Office/Counsellor Receives the SAR

When a SAR is received by the Organisation / counsellor from a Client or third party then the Office should follow the procedure below.

a) The Office emails the Client a **Consent to Disclose Form – Case Notes** which they are required to fill in, sign by hand and return to the Office.
b) The counsellor is required to provide the Office with a copy of the case notes for the client. The counsellor also needs to sign the **Consent to Disclose Form - Case Notes: Section B** to record the case notes have been provided to the Office and that this procedure has been completed.
c) If the SAR was received from the Client, rather than a third party, then the Office meets the Client in-person to give them the case notes. The Client must present 2 forms of ID, see **ID Summary Table for Client SAR** below, to the Office who records the details and any reference numbers on a **Confirmation of Receipt Form**, which is for Office use only. The Client signs by hand the Confirmation of Receipt Form to confirm they have received the case notes.
d) The Office does not need to retain copies of the client's presented ID or the counsellor's Client case notes.
e) If the SAR was received by a third party then the request must originate from a work-related email address.
f) The Office must meet the representative in-person. The representative must present 1 form of photographic ID to the Office that confirms the person's name and job title within the requesting organisation. Alternatively, they can present a letter from their work organisation which is on letter headed paper, states the details of the SAR and is signed by a senior member of staff. The Office records the details of the presented ID/signature on letter and any reference numbers on the Confirmation of Receipt Form.
g) The Office provides the case notes to the third party representative who signs by hand the Confirmation of Receipt Form to confirm they have received the case notes.
h) The Office does not need to retain copies of the representative's presented ID or the case notes.

i) The Office must provide the Client / third party with the case notes within 30 days from receipt of the SAR.

j) The Office maintains an audit trail of a SAR in the form of a **SAR Disclosure Record Sheet,** which is for Office use only, and details the dates of the initial request and the acknowledgement and provision of requested information. This in undertaken to ascertain whether or not the standard 30 days target was met, apart from any exceptions as specified above or if for example the counsellor for has left the Organisation potentially causing a delay in the provision of the case notes. If there were no exceptions and the standard target was not met, then the process is reviewed with the Centre Director and any short comings in the procedure are addressed.

k) All the SAR documents including the completed Consent to Disclose Form(s), Confirmation of Receipt Form and SAR Disclosure Record Sheet are saved on the Office electronic system, the completed hard copies are then shredded, and the electronic versions are saved for 3 years after which they are electronically deleted.

l) The counsellor should retain client case notes for 7 years from closure of contract and relevant SAR documents including; completed Consent to Disclose Form – Case Notes Form, case notes and any related correspondence, for 3 years from receipt of SAR, or for whichever is the longest time period eg., SAR received in the 5th year of case notes storage, plus 3 years for SAR documents, would be a total of 8 years of case notes storage, after which all these documents would be shredded or electronically deleted.

ID Summary Table for Client SAR

Consent to Disclose Forms	**Type of ID**	**Format of ID**	**How Requested Information is Provided**
Counselling Service Information	**Photo ID:** Passport/Driving Licence ***and*** **Proof of Address:** Utility bill, dated within last 6 months Council Tax Bill, dated within the last year	Original ID must be presented online via FaceTime or in-person and Office records details seen on the **Confirmation of Receipt Form**	Information requested may be sent via email, password protected, posted or collected in-person.
Case Notes	**Photo ID: For Example** Passport/Driving Licence ***and*** **Proof of Address:** Utility bill, dated within last 6 months Council Tax Bill, dated within the last year	Original ID must be provided in person and Office to record this and the details on **Confirmation of Receipt Form**	Case Notes must be collected in-person from the Office.

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 Data Controller 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
- Interception due to not having the right level of security in place when transmitting/transporting data.

Timeline Statement

The Member is then required to write a **Timeline Statement** regarding the breach of personal data and email this confidentially to 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 Data Controller and Service Support Manager review the Timeline Statement and together agree the contents of a **Summary Statement,** which is added to the statement, and details the required course of action the Member must implement. This will include a decision whether or not the breach of personal/special categories data is serious and as such if the Data Controller 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
Staff Review Documents Latest Year	Locked Cupboard/ On the Computer	6 Years after Leaving	Double Cross Shredder /Electronically Deleted
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/ On the Computer	3 Years	Double Cross Shredder /Electronically Deleted
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
Counsellors' Client Case Notes & SAR Docs	Locked Filing Cabinet	7 Years after Closure & 3 Years after SAR	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 All Relevant Docs	On the Computer	3 Years from SAR	Electronically Deleted
Student Placemts Reg Docs, Membership & Insurance	On the Computer	6 Years after Leaving	Electronically Deleted

29th March 2024