CLEAR emotional trauma & therapy specialists clearsupport.net | Reg charity no. 1165574		Name of Policy **Data Protection & Information Sharing Policy**
Author & Version	Date reviewed/approved	Signature of Chair
Andy Brelsford V2	December 2025	
Number of pages	8	Date of next review: December 2027

1. Purpose

This policy sets out how the charity acquires, processes, records, stores, discloses and destroys data in line with the Data Protection Act 2018 (DPA) and the UK's implementation of the General Data Protection Regulation (GDPR).

2. Scope

This policy is intended for:

- all members of the workforce (including trustees, staff, volunteers, students and contractors)
- service users

3. Related Documents

This policy should be read alongside:

- Data Protection Act 2018
- General Data Protection Regulation 2016/679
- Data Use and Access Act 2025
- The ICO guide to GDPR
- BACP Ethical Framework
- HCPC Standards of Conduct Performance and Ethics: https://www.hcpc-uk.org/standards/standards-of-conduct-performance-and-ethics/
- https://understandingpatientdata.org.uk/news/gdpr-and-patient-data

4. Definitions

For the purposes of this policy, the following definitions apply:

4.1 Service Users

The individuals who receive support from the charity. This includes survivors and their family or friends. The terms 'person', 'client' and 'victim' are also included in this definition.

4.2 Data Subjects

The individuals who the charity collects information on. This includes the workforce and service users, alongside contractors and suppliers of various kinds.

4.3 Personal and Sensitive Information

Data which can identify an individual and sensitive information includes the person's race or ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, the commission or alleged commission of any offences and details of criminal proceedings.

4.4 The Charity

For the purposes of this policy 'the charity' refers to CLEAR Emotional Trauma and Therapy Specialists

5. Background

The charity collects and uses information about the people with whom we deal. We also acquire information about others during those dealings. The information can be factual, such as name and address, or expressions of opinion about or intentions towards individuals and can be in any form or format (WORD documents, databases and spreadsheets, emails, index cards, paper files etc).

All the workforce and service users have an individual responsibility to uphold the legal requirements of the DPA and GDPR. Breaches may lead to disciplinary action being taken and, possibly, to prosecution of the individual concerned.

CLEAR is registered with the Information Commissioners Officer as a charity, and all individual therapists and counsellors are registered as individual practitioners. Registration will be maintained at all times.

6. Data Protection Principles

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. These principles are:

- Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless certain conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any matter incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7. Sensitive Data

The charity will collect and process sensitive personal data only when required to do so by law or when needed in connection with operational requirements. There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

8. Recruitment

Contracts and volunteer agreements make clear that individuals are bound by the provisions of the Data Protection Policy and that acceptance of the contract/completion of the training signifies consent to processing data. All members of staff, whether employed, sessional or volunteers are required to sign a Confidentiality Agreement (see Appendix B)

9. Security

All data held by the charity will be kept securely, whether kept by an individual or in the charity's offices. Any recorded information on service users or the workforce shall be:

- kept in locked cabinets; *or*
- protected by the use of passwords if kept electronically.

Access to information on a computer system is controlled by a password and only those needing access are given the password. Staff should be careful about the information that is displayed on a computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display. When transferring data electronically, consideration should be given to using encryption to protect the data should it be intercepted.

Anonymisation and pseudo- anonymisation of records may also give protection to data subjects so they cannot be identified from the computer records alone.

10. Retention of Data

The charity will only keep records containing personal sensitive data if they are relevant to the charity aims and objectives. The retention time will vary depending on the type of data. Unless contracts or grant agreements state otherwise documents will be retained securely as follows:

- Financial documents – 7 years following the end of the accounting period
- Employee records – 6 years following the end of employment
- Client documents (adults) – 6 years following the end of counselling/therapy
- Client documents (children) – until 25th birthday or following the end of therapy (whichever is the later)

Wherever possible data will be stored electronically in a secure database that requires secure access and login and is protected by a robust firewall.

11. Disposal of Data

When personal data is no longer to be retained it will be disposed of in such a way that the rights and privacy of the individual concerned are protected, e.g. disposal by shredding, burning, secure electronic deletion / disposal of hard drives and electronic storage devices

12. Publicly Available Information

The provisions of the DPA do not extend to information already in the public domain. Such information includes:

- Names of all members of the Management Committee.
- Name, initial(s), and job title as listed in various publications issued by the charity, e.g. training programmes, service directories, Awards and honours relating to work done for the charity.
- Information about the charity which is publicly available, including names of staff members.

13. Rights of Access to Data

Under the DPA you have the right to find out what information an organisation has about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

CLEAR will co-operate with any reasonable requests from data subjects (or their properly appointed representatives) to access any data we may hold on them in line with the DPA. In most cases CLEAR will not charge a fee for data subject requests. However, we may charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data. Any such request will be normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

The Freedom of Information Act (FOI) provides individuals and organisations with a right of access to information held by public services. Charities that deliver public services are however exempt from the Act and therefore CLEAR will not normally respond to any request for information under the FOI provisions.

14. Information Sharing

CLEAR will always ensure it has a lawful basis for the processing and sharing of data. The data subject shall be advised what information may be shared and the reasons why.

The data subject should be asked to consent to the sharing of their information. If the data subject is a child, the professional needs to be satisfied that the child understands what it means to consent or refuse the sharing of information. Consent may be given by another person on behalf of the data subject if they are not capable of exercising their rights independently.

Information may be shared without the consent of the data subject if:

- the sharing of information is required by law through a statutory duty or by a court order; *or*
- it is in the public interest to do so. For example, if seeking consent would place the data subject at risk of significant harm, prejudice the prevention, detection or prosecution of a serious crime or lead to an unjustifiable delay in making enquiries about allegations of significant harm to a child.
- There are serious and/or immediate safeguarding issues where we have reason to believe a child, young person or a vulnerable adult is at risk. Such cases will normally be discussed with a CLEAR Safeguarding Lead before any decision to share information is made (provided this does not involve any delay which might increase the risk).
- There are very specific issues around Pre-Trial therapy and the sharing of information. There are strict guidelines laid out about when and how we will share information in these circumstances. (See CLEAR's Pre-trial Therapy Policy)

The facts of the individual case should be considered when deciding whether to share information without consent. The safeguarding of the individuals involved should be the main consideration. Guidance on making this decision can be found in Appendix A and the ICO website.

The discussions and consent or refusal to share information shall be recorded in writing. Information must be accurate and necessary for the purpose for which it is being shared and shared only with those who need to see it.

15. Data Breaches

In the event that CLEAR inadvertently shares data inappropriately, we will:

- Notify the data subject(s) at the earliest opportunity
- Conduct an investigation with senior leadership involvement to understand what happened, how and why
- Report back to any data subject(s) affected by the breach on the investigation, its progress and its findings
- Understand what the data subject(s) would like to happen next and take appropriate steps to facilitate this where possible
- Notify our Management Team, Trustees and/or the ICO (as appropriate) of the breach and identify what steps we need to take and implement those steps to prevent a recurrence.

16. Other Complaints

CLEAR has a process for anyone who wishes to make a complaint about how we process, store or share their information. Details can be found on our website. We will acknowledge all such complaints within 30 days and respond without undue delay. We will also support complainants through the process, where requested.

Appendix A – Decision Checklist

The below considerations may assist with the decision about whether to share information. The safeguarding of the data subject should be the primary consideration in all decision making about information sharing.

The below checklist is sourced from the Information Commissioner's Office, Data Sharing Checklists, licensed under the Open Government Licence.

1. Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

2. Do you have the power to share?

Key points to consider:

- The type of charity you work for.
- Any relevant functions or powers of your charity.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

3. If you decide to share

Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

4. Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information. If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Appendix B – Confidentiality Agreement

This is to certify that I [Name], in my capacity of [Role] understand that any information (written, verbal or other forms, intellectual property, licensed) obtained during the performance of my duties must remain confidential and returned if employment/engagement is ceased.

This includes all information about members, clients, families, employees and other associate organisations, as well as any other information otherwise marked or known to be confidential.

I understand that any unauthorised release or carelessness in the handling of this confidential information is considered a breach of the duty to maintain confidentiality.

I further understand that any breach of the duty to maintain confidentiality could be grounds for immediate dismissal and/or possible liability in any legal action arising from such breach. I understand that CLEAR adheres to the BACP ethical framework in terms of client confidentiality.

_____

Your Signature

_____ Date

Signature of Chief Executive Officer

_____ Date

Appendix C – BACP Ethical Framework: Data Protection

- Practitioners are advised to keep appropriate records of their work with clients unless there are good and sufficient reasons for not keeping any records.
- All records should be accurate, respectful of clients and colleagues and protected from unauthorised disclosure.
- Any records should be kept securely and adequately protected from unauthorised intrusion or disclosure.
- Practitioners should take into account their responsibilities and their clients' rights under data protection legislation and any other legal requirements.
- Respecting clients' privacy and confidentiality are fundamental requirements for keeping trust and respecting client autonomy.
- The professional management of confidentiality concerns the protection of personally identifiable and sensitive information from unauthorised disclosure.
- Disclosure may be authorised by client consent or the law.
- Any disclosures of client confidences should be undertaken in ways that best protect the client's trust and respect client autonomy.
- Communications made on the basis of client consent do not constitute a breach of confidentiality. Client consent is the ethically preferred way of resolving any dilemmas over confidentiality.
- Exceptional circumstances may prevent the practitioner from seeking client consent to a breach of confidence due to the urgency and seriousness of the situation, for example, preventing the client causing serious harm to self or others. In such circumstances the practitioner has an ethical responsibility to act in ways, which balance the client's right to confidentiality against the need to communicate with others.
- Practitioners should expect to be ethically accountable for any breach of confidentiality.
- Confidential information about clients may be shared within teams where the client has consented or knowingly accepted a service on this basis; the information can be adequately protected from unauthorised further disclosures; and the disclosure enhances the quality of service available to clients or improves service delivery.
- Practitioners should be willing to be accountable to their clients and to their profession for their management of confidentiality in general and particularly for any disclosures made without their client's consent.
- Good records of existing policy and practice and of situations where the practitioner has breached confidentiality without client consent, greatly assist ethical accountability.
- In some situations, the law forbids the practitioner informing the client that confidential information has been passed to the authorities, nonetheless the practitioner remains ethically accountable to colleagues and the profession.