



The Guild of Psychotherapists

Data Management Policy and Guidance

JUNE 2026

POLICY OWNER:	Senior Administrator
Dates of Approval	
Approved by Policy Committee	March 2025
Approved by Council	April 2025
Reviewed	June 2026
Locations	
Places on Sharepoint and website where this policy is stored and need to be replaced by subsequent versions	• Sharepoint policy folder • Members area of website • Public website
Review Frequency	Annually
Next Review Date	2027

This document contains both the Guild's Data Management Policy (including data retention and privacy) Procedures to make Data Management Complaints and for use in the event of a Data Breach.

The Policy should be reviewed according to the Policy Review cycle.

Contents

Section A: The Guild's Data Management Policy

1. Introduction and Purpose
2. Definitions
3. Applicability and Scope
4. Statutory and Regulatory Requirements
5. Responsibilities for Compliance
6. Communication and Training
7. Monitoring and Auditing

Section B: The Guild's Commitments

1. The Guild's Commitment to Data Protection
2. The Guild's Commitment to upholding the rights of individual data subjects

Appendix 1: Data Retention Schedule

Appendix 2: Guild Personal Data Breach Procedure

Appendix 3: Data Management Complaints Procedure

Appendix 4: Subject Access Request Procedure

Section A: Data Management Policy

1. Introduction and Purpose

The responsible handling of data is of paramount importance to the Guild, as a psychotherapeutic organisation that by its nature works with highly sensitive information. The lawful and appropriate management of records and personal data is a legal and regulatory requirement as well as an important ethical value. This policy sets out our commitment to protecting personal data, with reference to its collection, use and disposal.

We aim to promote the adoption of good practice and foster the implementation of a safe culture of privacy across the organisation. The Guild needs to collect data in the course of its work and is the decision-maker when it comes to how people's personal information is collected, handled and stored. The Guild is therefore a 'data controller' as defined by the Information Commissioner's Office (ICO). We aim to follow the principles outlined by the ICO, which state that personal data must be:

- Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes ('purpose limitation')
- Adequate, relevant and limited to what is necessary to the purpose for which they were obtained ('data minimisation')
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay ('accuracy')
- Kept for no longer than is necessary ('storage limitation principle')
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage ('integrity and confidentiality')

The Guild is permitted to handle only that data for which it has a valid, lawful basis on which to do so; this usually means that it is necessary in order to provide services.

Our commitments and responsibilities are set out more fully in Section B.

2. Definitions

- The term 'member' denotes all practising and non-practising Guild members.
- The term 'trainee' denotes all of those participating in any of the Guild's programmes, including the clinical training programme, supervision programme and short courses.
- Other personnel include staff, external (non-member) trainers and speakers, whether on a voluntary or paid/contracted basis, and any other contractors employed by the Guild or volunteers involved in the management of Guild systems or premises.

3. Applicability and Scope

The policy applies to all personal data that the Guild holds or has control over which relate to the provision of the organisation's core services, ie the low-fee clinic, education and training, membership etc. It does not apply to data relating to the internal management of the Guild, such as employment, procurement etc, which will be outlined in a separate document.

The data referred to in this policy include physical data, such as hard copy documents, contracts, notebooks, letters, invoices etc. It also includes electronic data, such as emails and electronic documents (audio and video recordings).

The policy applies to all personal data that the Guild holds in relation to living identifiable individuals regardless of the category or format of the data. Personal data refers to any data which could be used to identify a living individual e.g. name, address, email, postcode, photograph etc. 'Special categories' of personal data refers to any information about racial or ethnic origin, religious beliefs, health (mental and physical), sexual health, sexual orientation or gender identification and criminal convictions.

The policy applies to personal data held or accessed on Guild premises and to personal data that is accessed remotely or stored on personal and removable devices in the course of the legitimate business of the organisation.

Responsibility to implement this policy applies to all staff, members, trainees, contractors and visitors. The policy applies to work carried out within the Guild premises and/or in the course of duties, responsibilities and engagement with carrying out the Guild's core objectives (e.g. teaching, recruiting, working in the low-fee clinic, sitting on Guild committees etc.) and participating in Guild activities.

This policy does *not* relate to the private clinical practices of members and trainees. However, all practitioners in private practice are also required to comply with data management principles and regulations, therefore this policy will speak to how people practise privately. The Guild expects its members and trainees to ensure they practise safely and to consult the guidance provided by the UKCP and the Information Commissioner's Office, with regard to the relevant legislation:

[ukcp-security-and-confidentiality-guidelines-2018-june2024.pdf](#)
[Advice for small organisations | ICO](#)

All practising members and trainees are expected to take out professional indemnity/civil liability insurance that covers claims for the loss of personal data.

Guild personnel have mutual responsibility towards each other, each individual and group to safeguard the privacy of others as data subjects in their own rights. The Guild will also ask that confidentiality be observed by visitors to the Guild, such as anyone using Guild services or attending the premises, including: non-members attending Guild events, such as conferences and lectures; prospective trainees attending open days, induction days and interviews; clients using the services of the low-fee clinic. The Guild in turn has a responsibility to protect the confidentiality of all the aforementioned categories of personnel.

4. Statutory and Regulatory Requirements

The Guild's implementation of the Data Management Policy and associated procedures are intended to ensure full compliance with the following Regulations:

- General Data Protection Regulations (GDPR)
- UK Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)

5. Responsibilities for Compliance

The Guild of Psychotherapists places responsibilities for compliance with personnel at all levels. All employees, member and trainee psychotherapists, volunteers and advisors, contractors and visitors have a

responsibility to ensure personal data is collected, stored, handled and processed in accordance with this policy. Failure of the Guild to comply can expose us to penalties, difficulties providing information when required and reputational damage; it is therefore the responsibility of everyone to understand and comply with the policy. Failure by personnel to comply may result in disciplinary sanctions.

The Council

The Trustees are ultimately responsible for ensuring that the Guild meets its legal obligations. They delegate:

- Responsibility for oversight of the Policy to the Data Protection Link Trustee in consultation with Officers, Senior Administrator and Chairs of Standing Committees
- Responsibility for the day-to-day implementation of the Policy to the Data Protection Officer.

Data Protection Officer

The Guild appoints the Senior Administrator as Data Protection Officer (DPO), who is responsible for:

- administering the data protection management programme and monitoring compliance
- developing data disposal policies, systems, standards and procedures
- providing guidance and training
- managing data breaches and data subject rights
- recording and maintaining appropriate records of processing activities and evidence of monitoring
- putting into practice in conjunction with other staff who are responsible for data management within their specific areas of The Guild, such as Training and the Clinic.

The DPO should consult the Data Management link Trustee for advice/queries.

6. Communication and Training

Staff Training

All staff will be made aware of good practice in data protection and where to find guidance and support for data protection issues. Training appropriate to role will be available to ensure all personnel understand their responsibilities when handling data. Personal data will only be accessible to those authorised to know it, on a 'need to know' basis.

Trainees and Members

Trainees and members will be made aware of their responsibilities with regard to data management. Information will be provided at the point of induction to new trainees and regular reminders will be given to members via Guild communications. Trainees and members will be able to consult the DPO or Council Officers with any problems or queries. Data Management will be included in the trainee induction to working in the Guild low-fee clinic. The full data management policy will be available in the members' area of the Guild website.

External Personnel

External personnel working with the Guild will be reminded of their responsibilities and given access to the Data Management Policy.

Communication to the Public

This document will be made available to members of the public on request. In addition, a detailed privacy policy will be posted on the Guild website to assure the public of the Guild's commitment to responsibly managing the data collected from anyone using its services.

7. Monitoring and Auditing

Regular audits will be undertaken (by the DPO) to ensure compliance with the law, with this policy and any relevant procedures. This policy will be reviewed annually by the Guild Council; Council will also review any data protection incidents, weaknesses, breaches, also changes required by legislation or changes within the organisation. If such reviews result in the need for modification of the policy, this will be carried out immediately and all personnel will be informed.

SECTION B: The Guild's Commitments

1. The Guild's Commitment to Data Protection

The Guild will comply with legal obligations and the ICO's data protection principles by:

Processing with Transparency, Lawfulness and Fairness:

We will ensure that the Guild processes personal and special category data in accordance with the legislation. Where data subjects' consent is required to process personal data, this will be requested in an intelligible and accessible manner. Data subjects will be advised of their right to withdraw consent and the process for withdrawing consent will be straightforward.

Purposes

Personal data will only be used for the original purpose for which it was collected and this purpose will be made clear. If the Guild wishes to use personal data for another purpose, we will notify the data subject prior to processing.

Adequate and Relevant Data

The Guild will only collect the minimum data required for the purpose. Any data found to be either in excess of this or no longer required for the purpose it was collected for will be securely deleted. Any personal data that is optional for individuals to provide will be clearly identified as such.

Accuracy

The Guild will take reasonable steps to keep personal data up to date. Any data found to be inaccurate will be updated promptly, including any inaccurate data that has been shared with third parties.

Retention and Disposal

The Guild will hold data for the minimum time necessary to fulfil its purpose.
Please see Appendix 1 for further details of how long data is retained.

Security

The Guild will implement appropriate security measures to protect personal data and all personnel will keep data secure by taking sensible precautions. Examples would include keeping data recorded on paper in locked filing cabinets, drawers or offices; ensuring care is taken whenever data is transferred, for example not losing documents or memory sticks and using passwords when emailing identifiable data.

Data Sharing

There are certain circumstances in which the Guild may share personal data with third parties, including rare circumstances in which this may be done without consent, such as in unexpected and emergency situations. Appropriate security measures will be used when sharing any personal data.

Data Processors

Where the Guild uses 3rd party data processors, that is to say outside providers such as website hosts, we will ensure that they have appropriate security measures in place, adequate technical measures and that there is a contract explaining what is required of the data processor.

Security Incident & Breach Management

All security incidents or personal data breaches will be reported and managed by the Guild's DPO, who will inform the Chair and the Trustees. The Information Commissioner's Office and the individuals affected will be notified promptly, if required. All breaches will be managed using the Guild's Personal Data Breach Procedure (see Appendix 4).

Any breaches of this policy may be considered under the Guild's disciplinary procedures and may result in disciplinary action.

Building in Privacy

The Guild has an obligation to implement measures to demonstrate we have considered and integrated data protection throughout the organisation's activities. Trustees are responsible for ensuring that data audit is completed, as required by Article 30 of GDPR, which sets out exact documentation requirements for data controllers.

2. The Guild's Commitment to Upholding the Rights of Individual Data Subjects

The Guild will uphold the rights of data subjects to access and retain control over their personal data held by us.

- **Right to access** – by ensuring individuals are aware of their right to know how their data is being processed, their right to access their personal data and how to exercise these rights. (See Appendix 3 for subject access request procedure).
- **Right to be informed** – about how and why their data is used. This information should be available in an accessible, transparent and timely way.
- **Right to have their data rectified** – by correcting, in a timely way, any personal data that either changes or is found to be inaccurate. Data subjects will be advised of how to inform us of inaccuracies.
- **Right to erasure** – data subjects will be advised on their right to request deletion or removal of personal data where processing is no longer required or justified.
- **Right to restriction** – we will restrict processing of data when a valid request is received and will inform individuals of how to access this right.
- **Right to object or withdraw consent** – we will stop processing personal data if requested, unless we can demonstrate legitimate grounds for processing, which override the interest, rights and freedoms of the individual or if the processing relates to the defence of legal claims. Individuals should be aware that there may be circumstances in which we will not be able to provide services without consent to process certain data.
- **Right to portability** – enabling, where possible and appropriate, data to be transferred to a similar organisation.
- **Right not to be subject to automated decision-making** – the Guild does not make decisions without human involvement.

Appendix 1: DATA RETENTION SCHEDULE

In accordance with ICO requirements:

- we only keep personal data as long as is reasonable and necessary for the purpose for which it was collected.
- we carefully consider and can justify how long we keep personal data. This may include the fulfilling of statutory obligations or to satisfy any legal, accounting or reporting requirements.
- we regularly review our information and erase or anonymise personal data when we no longer need it
- we only use data that is anonymised, when we provide information for research or statistical purposes (Note that pseudonymised data, such as coded CORE forms, provides additional security measure to reduce risk to data subjects but since it can be identified, it remains personal data.)
- we regularly review the retention schedule so it continues to meet legal requirements and we update it quickly when a change is required

It is not possible to identify and list every type of data; below are our guidelines for some of the broad categories. However, in accordance with the above principles, we make reasonable and proportionate decisions in respect of all personal data that the Guild handles.

LOW FEE CLINIC

For people who apply to the low fee clinic but do not proceed to become clients in the clinic, we will retain initial contact and assessment forms for 1 year, after which they will be securely destroyed.

For clients who proceed to the low fee clinic, we will retain records for 2 years after the end of treatment, after which they will be securely destroyed. This will include all records held by the Guild in managing the provision of therapy, for example initial, assessment and closing forms, correspondence between clinic staff and clients, admin records such as invoices and attendance records. This period allows for concerns, complaints, safeguarding issues etc that may arise after the client's engagement with the clinic has ended.

TRAINING

Trainee records are maintained for a period of 10 years after the completion or termination of training.

MEMBERS

Members' details will be held for a period of 6 years after termination of membership.

COMPLAINT AND SUBJECT ACCESS RECORDS

Maintained for a period of 10 years after resolution or completion.

Appendix 2: SUBJECT ACCESS REQUEST PROCEDURE

By law, people can ask for a copy of any information held by an organisation, that's to do with them; it's their personal data and they have the right to see it. A request can be made verbally, online, in writing or via a third party; this is a 'subject access request' (SAR), and as a data controller, the organisation has a legal obligation to respond. Requests made to the Guild will be dealt with by the DPO and in accordance with the ICO's guidance.

For the public:

- Anyone can make an SAR, you don't need a lawyer or solicitor
 - The quickest way to do this is to email the Guild at:
DataProtection@guildofpsychotherapists.org.uk
- You can use optional template available on the ICO website to write your SAR.

On receipt of a SAR, the Guild will:

- Acknowledge the request straight away
- Ask for further information as soon as possible if this is needed
- Respond with transparency and ensure there are no barriers to valid requests
- Help data subjects who need support with their request
- Verify the identity of the requester or make sure the request is valid if made by a 3rd party
- Check carefully what has been requested, as it may not necessarily comprise all data held
- Perform a reasonable search for the information that has been requested
- Consider carefully if 3rd party information would be included in the disclosure and whether redaction or withholding of any information is needed
- If an exemption can be applied (e.g. for legal reasons), consider each case on its merits and seek to disclose information where possible
- Respond within a month (this can be extended to 2 months in some circumstances)
- Provide the information in an accessible and intelligible format
- Disclose the information securely and keep a record of what has been provided
- Comply with the request free of charge, except in certain circumstances, such as excessive or duplicated requests where a reasonable administrative fee will be charged

Erasure:

Data subjects can also contact the Guild at the above address to request erasure of their data, known as the 'right to be forgotten'. As with SARs, the request can be made verbally or in writing and the organisation has a month to respond. The right is not absolute and only applies in certain circumstances, however the Guild will endeavour to comply with all reasonable requests.

Appendix 3: DATA MANAGEMENT COMPLAINTS PROCEDURE

1. Introduction

The UK General Data Protection Regulation (“UK GDPR”), the Data Protection Act 2018 (“DPA 2018”), and the Privacy and Electronic Communications Regulations (“PECR”) (together, the “Data Protection legislation”), give data subjects and applicable third parties rights in relation to personal data. This procedure details how The Guild will respond to complaints from data subjects and third parties relating to the use of personal data

Who are Data Subjects?

Data subjects are any natural living individuals whose personal data the Guild processes (collects, obtains, stores, retains, disposes of etc.). Data subjects can include staff, members, trainees, applicants, prospective applicants, clinic patients, seminar leaders, guests, visitors, etc.

Data subjects’ rights

Under Data Protection legislation, data subjects have the right to the following and these rights can be exercised at any time:

- a. information about the processing of their data (UK GDPR Articles 12-14, and Recitals 58-62),
- b. access their own personal data (UK GDPR Articles 12 and 15, and Recital 63),
- c. correct personal data (UK GDPR Article 16),
- d. erase personal data, also known as the right to be forgotten (UK GDPR Article 17, and Recitals 65 and 66),
- e. restrict data processing (UK GDPR Article 18),
- f. object to data processing, including direct marketing (UK GDPR Article 21, and Recitals 69 and 70),
- g. receive a copy of their personal data or transfer their personal data to another data controller (data portability, UK GDPR Article 20, and Recital 68),
- h. not be subject to automated decision-making and rights in relation to profiling (UK GDPR Article 22, and Recital 71), and
- i. be notified of a data security breach (UK GDPR Article 34, and Recital 86).

What is a complaint?

A complaint is an expression of dissatisfaction about The Guild’s handling of a data subject’s personal data or the data of the individual they represent. This can also include dissatisfaction with how The Guild has responded to a previous data request, such as those detailed in the section on Data Subject’s Rights above.

2. Scope

This procedure addresses complaints made by data subjects regarding the use of their personal data. Complaints may be made in relation to any aspect of The Guild's processing of personal data including individual rights requests.

This procedure also addresses complaints made by third parties in relation to The Guild's use of personal data. These may be for example in relation to The Guild's response to a data related request from a third party, such as the Police or Local Government Agencies.

This procedure should also be followed for complaints in relation to use of personal data for direct marketing and/or profiling activity.

3. Responsibilities

The Trustees have overall responsibility for this procedure but have delegated day-to-day responsibility for overseeing its implementation to the Data Protection Officer. All relevant members of staff have been made aware of the procedure and have received appropriate training.

All Employees are responsible for ensuring that any complaints that are made in relation to this procedure are reported to the Data Protection Officer, and for cooperating with the Data Protection Officer in reviewing these complaints.

The Data Protection Officer, Trustees (and The Guild's solicitor as required) will review this procedure from time to time to ensure that its provisions continue to meet our legal obligations and reflect best practice.

4. Making a Complaint

Data subjects and third parties may make a complaint relating to The Guild's use of personal data. Complaints should be sent directly to the Data Protection Officer's email: DataProtection@guildofpsychotherapists.org.uk.

The Data Protection Officer will normally acknowledge the complaint within 10 working days. The Guild reserves the right to extend the period for response during vacation and Guild closure.

Although a complaint may be brought at any time, there may be limits as to what The Guild can do in historic cases.

The Guild will only accept a complaint from a data subject's representative, if the representative provides the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint.

If there is any doubt about the identity of the complainant, the Data Protection Officer will first seek to verify the data subject's identity or third party's entitlement to act on behalf of the individual. The forms of identification that are acceptable from a data subject are as follows;

- a. Passport
- b. Driving Licence
- c. For third parties the identification requirements will vary dependent on their relationship to the data subject, and these will therefore be assessed on a case by case basis.

5. Investigation and Complaint Outcome

Once all identification requirements have been met, the investigation will be carried out without undue delay and complainants will be kept informed of the progress of investigation. If further clarification is required from the complainant for the response to be completed The Guild will inform the complainant.

In order to respond to the complaint, the investigation may necessitate access to personal data and other information held across the Guild. The cooperation of any staff members able to assist with the investigation will be required. The reason for the investigation may need to be disclosed to the relevant staff and Guild members.

The complaint outcome will be communicated to the complainant in writing, normally by email.

6. Review

If the complainant does not agree with the outcome, they can request a review of the decision. This request must be made within 1 month of the original decision being communicated and should be sent to the Data Protection Officer's email: DataProtection@guildofpsychotherapists.org.uk.

The decision will be internally reviewed by the Data Protection Officer or Trustees without undue delay from the receipt of the request for Review.

Once the internal review has been completed, The Guild will communicate the outcome in writing, normally by email.

7. Independent External Review

If the complainant remains dissatisfied, they can escalate their complaint to the Information Commissioner's Office (the "ICO"). Information about how to make a complaint to the ICO can be found here: <https://ico.org.uk/make-a-complaint>

8. Manifestly unfounded, abusive, vexatious or excessive correspondence and complaints

Independent External Review

In some scenarios we can refuse to handle the complaint. This will be when a complaint is deemed to be manifestly unfounded, abusive, vexatious or excessive. Each complaint will be considered on a case by case basis. The following factors will be taken into consideration:

- a. the data subject has explicitly stated that they intend to cause disruption (whether in the complaint, or in other correspondence), and has threatened individuals;
- b. the data subject has made unsubstantiated accusations against individuals, and is persisting in those accusations;
- c. the data subject is targeting particular individuals, against whom they have a personal grudge;
- d. the data subject makes frequent complaints intended to cause disruption; and
- e. the data subject continues to repeat the substance of previous complaints which have already been investigated.

Where a complaint is deemed to be manifestly unfounded, excessive, abusive or vexatious The Guild will contact the individual and in a reasonable timeframe explain to them:

- a. the reasons for refusing to consider the complaint;
- b. their right to make a complaint to the ICO; and
- c. their right to pursue their data subject rights through a judicial remedy.

9. Use of Data from Complaints

The Guild will collect data on complaint outcomes at each stage of this procedure and any complaints submitted by complainants to any regulators (including the ICO), and use the data:
a) internally for reporting, evaluation, learning and training; and b) externally for discussion with regulators

The data used by The Guild for these purposes will be anonymised. Your personal data and sensitive personal data ('Personal Data') as defined by the Data Protection Act 2018 (the "DPA") may be disclosed to The Guild's members of staff and regulators only for the purpose of dealing with your complaint, or a complaint arising out of it and/or implementing any recommendations. Personal Data will not be shared with any other third parties unless the Guild has your express consent, has a statutory obligation to do so, or is otherwise permitted to do so under the DPA.

Appendix 4: DATA BREACH PROCEDURE

The Guild will take every precaution to keep personal data safe. However, it is possible that a data breach could occur, for example if a document or equipment misplaced or lost due to human error, if data is stolen, accidentally disclosed or inappropriately accessed. In the event that any breach happens, the Guild will respond as follows.

Staff will promptly report the breach to the DPO, who will manage the incident.

The DPO will:

- Inform the Data Management Link Trustee and the Chair of the Guild
- Work out what has happened and who has been affected
- Assess the risk to those affected and act to protect them where necessary
- Notify, without undue delay, affected individual data subjects who may not already be aware
- Take steps to minimise the risk, including providing advice to data subjects on how to protect themselves from the effects of the breach
- Contain the breach where possible
- In consultation with the Guild Officers, take a decision on whether the breach meets the threshold of reporting to the ICO. If so, this must be done within 72 hours of becoming aware of the breach, where feasible
- Investigate the causes of the breach and report to Council with a plan to minimise the risk of future breaches
- Keep a record of breaches of personal data, irrespective of whether they require notifying the ICO
- Implement training or disciplinary action in respect of personnel who may have caused the breach