



DATA PROTECTION POLICY

1. Purpose

To provide an overview of our Data Protection Policy and procedures relating to how we protect staff and trainee data.

2. Scope

The people responsible for this Data Protection Policy are Susie Hewitt (Founder and Director) and Katie Gill (Academic Administrator) - collectively known as the Management Team.

This Policy applies to all employees, consultants and external trainers (the staff) who handle data relating to the Psychotherapy Institute (the Institute).

3. Background

3.1 The Institute is registered with the ICO with Registration Number ZB789535.

3.2 The Institute is Data Controller for personal data relating to the following groups of people:-

- Trainees on our 4-year Training
- Applicants to our 4-year Training
- External Trainers
- Employees
- Consultants
- Delegates
- People who enquire about our training or courses
- Job applicants

3.3 As per our Privacy Notice we process data for the following purposes:-

- Student education and welfare
- Queries, complaints or claims
- Information updates or marketing purposes
- Recruitment
- Employment processes and procedures



	3.4	The legal basis for processing each of the above purpose categories, is as follows:- • Student education and welfare – consent and contract • Queries, complaints or claims – contract • Information updates or marketing purposes – legitimate interests • Recruitment – legitimate interests
4.	Our Privacy Notice	
	We have a Privacy Notice that is made available to via our website.	
5.	Our Policy on Cookies	
	Psychotherapy Institute – Cookie Policy Psychotherapy Institute (“we”, “us”, “our”) uses cookies and similar technologies on our website (www.psychotherapyinstitute.co.uk) to ensure the site functions effectively, to improve your experience, and—only with your consent—to help us understand how our website is used. This Cookie Policy explains what cookies are, which types we use, why we use them, and how you can control your cookie preferences. It should be read alongside our Data Protection & Privacy Policy, which explains how we handle personal data in line with the UK GDPR and the Data Protection Act 2018.	
	a. What Are Cookies? Cookies are small text files that are placed on your device (computer, smartphone, or tablet) when you visit a website. They help websites remember your actions and preferences over time. Cookies that identify you or are capable of doing so are considered “personal data” and must be handled in accordance with UK GDPR and PECR.	
	b. Types of Cookies We Use We use the following categories of cookies: Strictly Necessary Cookies (Essential) • Required for the website to function properly. • Enable core features such as page navigation, security, and access to private areas of the site (e.g., booking systems). • These cookies do not require consent, but you will be informed about them.	



Functionality Cookies

- Allow the website to remember choices you make (such as language preferences).
- Support an improved and personalised user experience.

Performance and Analytics Cookies

- Collect anonymous data about how visitors use our website (e.g., which pages are visited most often).
- We may use tools such as Google Analytics, configured in accordance with ICO guidance to minimise data collection.
- These cookies are **only set with your consent**.

Third-Party Cookies

- Some third-party services embedded in our site (e.g., appointment booking systems, embedded videos, or social media links) may set their own cookies.
- These cookies are controlled by the relevant third party; more information can be found in their respective privacy/cookie policies.

c. How We Obtain Consent

For all non-essential cookies, we will:

- Ask for your clear, informed consent via a cookie banner or pop-up when you first visit the site.
- Allow you to accept or reject non-essential cookies.
- Provide an option to manage or change your consent at any time.

We do **not** use pre-ticked boxes or assume consent through continued browsing.

d. Managing Cookies

You can manage your cookie preferences at any time by:

- Adjusting the cookie settings available on our website.
- Changing your browser settings to block or delete cookies.

Please note:

- Disabling essential cookies may affect the functionality of the site.
- Instructions for managing cookies in common browsers can be found on the ICO website or via your browser's help pages.

e. How Long Cookies Are Stored

Cookies may be stored for:

- **Session** duration (deleted when you close your browser), or
- **Persistent** periods (remaining on your device until they expire or you delete them).

We only retain cookies for as long as necessary for the purposes described above.

f. Personal Data and Cookies

Where cookies collect personal data, such processing is conducted in accordance with:

- The **UK GDPR**,



	• The Data Protection Act 2018, and • Our Data Protection & Privacy Policy. Our lawful basis for using essential cookies is legitimate interests or performance of a contract. Our lawful basis for using non-essential cookies is your consent.	
	g. Updates to This Cookie Policy We may update this Cookie Policy from time to time to reflect changes to laws, guidance, or our practices. Updates will be posted on this page with an amended “last updated” date.	
	h. Contact Us If you have questions about this Cookie Policy or our data protection practices, please contact: Psychotherapy Institute Email: office@psychotherapyinstitute.co.uk	
6.	Our Data Retention Policy	
	We maintain a separate Policy that details how long we retain data for (which may vary depending on the nature of the data and the basis of processing).	
7.	Data Breaches	
	7.1	In accordance with UK GDPR a data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
	7.2	A data breach can occur accidentally or can be deliberate.
	7.3	We understand that we have a duty under UK GDPR to report certain personal data breaches to the ICO within 72 hours of becoming aware of the breach, when possible.
	7.4	We also understand that we are required – where a breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms – to inform those individuals without undue delay.
	7.5	In the event of any member of staff becoming aware of a data breach, they must immediately report the breach to a member of the Management Team via the office inbox.



	7.6	The breach report will be investigated without delay by the Management Team who will advise of any further steps to be taken with regards to the breach.
	7.7	Where it is deemed necessary a report will be made to the ICO as per the Regulations and to the individuals affected if it is decided that they are at high risk (as per the above wording).
	7.8	The Management Team will maintain a Breach Register to record all reported breaches whether it was deemed necessary to report to the ICO/ individuals affected or not.
8.	Data Subject Rights	
	8.1	Data Subjects (i.e. individuals for whom we hold their personal data) have various rights under UK GDPR. These include:- • Right to rectification • Right to erasure • Right to restriction of processing • Right to object to processing • Right to data portability • Right to withdraw consent
	8.2	Where we are notified that a Data Subject wishes to exercise one or more of their above rights we will endeavour to comply with a request to the best of our ability. However, each request will be considered carefully and on a case-by-case basis by the Management Team to evaluate the extent to which we can comply with such a request.
	8.3	Our initial investigation into the request may include assessing whether one of the exemptions under UK GDPR applies.
	8.4	Where we are restricted in our ability to comply with a request (in part or in full) but we do not believe an exemption applies we will seek further guidance from the ICO and ensure that the Data Subject is kept informed and advised that we are dealing with their request but seeking some further clarification from our Regulator.
	8.5	In the event of an exemption applying to the circumstances of the request we will ensure that the Data Subject is advised accordingly and that such a response is sent within good time and in accordance with any time limits set by UK GDPR.



	8.6	Where a Data Subject Access Request (DSAR) is made we will comply with such requests within the timeframe prescribed by UK GDPR. However, if we are unable to provide the data within the timeframe (within one month of the DSAR being made) we will ensure that the Data Subject is advised of the delay and the reasons why we have been unable to comply with the timeframe.
	8.7	We will ensure that the full process from receipt of a Data Subject request through to conclusion of dealing with the request is fully documented.