OPERATING POLICIES

Gateway Psychology Operating Policies are statements on the way Gateway Psychology will operate within the Business System. They signal the values and philosophy of our Company and provide a framework of general principles for all employees, Associates and colleagues to follow.

Contents

SIGNATORIES (signed and controlled electronically)

Dr Meryl Ann Forse
Dr M.A. Forse – Managing and Clinical Director

Confidential. This document is the property of Gateway Psychology Ltd.
This is an electronic document. Paper copies may not be the latest version.

1. SCOPE OF POLICY

This policy applies to all worker, this includes Employees, Contracted Associates, agency workers and service contractors ("Staff") of Gateway Psychology ("the Company").

2.0 WHY WE NEED A POLICY

Since the Company holds and processes sensitive personal and confidential information on individuals ("personal data"), we need to comply with UK's Data Protection Act 1998, the EU General Data Protection Regulation (GDPR) and Data Protection (Processing of Sensitive Personal Data) Order 2000 ("the Act"), as well as fulfil our professional and ethical responsibilities as defined by the HCPC and other professional and statutory bodies. Consideration also needs to be given to the requirements of the Freedom of Information Act 2000.
Further information can be obtained from the UK Information Commissioner's Office (website http://www.ico.org.uk/).

3.0 KEY MANAGEMENT RESPONSIBILITIES

3.1 Understand current and new policies, and the role of management with respect to them.
3.2 Ensure that all employees, Associates and contractors understand current and new policies through communication and familiarisation, and behave in accordance with them.
3.3 Actively work to ensure that Gateway Psychology Policies are maintained and developed, through reviewing their own policies and processes and receiving and monitoring feedback information.
3.4 Monitor the policy locally and eradicate any non-conformances that may be identified.
3.5 Agree and contribute to the development of new policies and processes where applicable, and when agreed, commit to implement those policies and processes.
3.5 Gateway Psychology Managers are responsible for the continual monitoring and improvement of Policies and Processes for which they have responsibility.
3.6 Ensure that any concerns raised with Policies or Processes are directed to the manager within the relevant function.

4.0 DETAILS OF THE POLICY

4.1 The Company will register that it records, stores and processes personal data with the UK Information Commissioner's Office ("ICO").

4.2 The Company will handle, store and process data of individuals both fairly and lawfully. ["Processing" means collecting, using, disclosing, retaining or disposing of personal data].

This means that the Company:

- Has legitimate reasons for collecting and using the personal data;
- Does not use the data in ways that have unjustified adverse effects on the individuals concerned;
- Is open, honest and transparent about how we intend to use the data;
- Gives individuals appropriate privacy notices when collecting their personal data;
- Processes people's personal data only in ways they would reasonably expect;
- Ensures that the Company does not do anything unlawful with the data;
- Ensure that the individual explicitly consents to the Company processing their sensitive personal data (unless this requirement is exempt in the Act or required for legal or statutory purposes). Consent may be withdrawn at any stage.

4.3 The Company will notify individuals (especially clients) about information that will be processed and held about them, gain consent and inform what will be done with this data.

4.4 In particular, since the Company is involved with psychological assessments, therapies and in some cases, acting as Expert Witnesses in Court proceedings, sensitive personal data (both factual and professional opinions where relevant) may consist of:

- Medical records
- Mental health records
- Social care records
- Criminal and/or court proceedings
- Attorney and legal counsel records and letters
- School and educational establishment records
- Clinical notes from sessions held with the client
- etc.

The purpose of collecting and processing such data is in order to fulfil the Company's professional psychological obligations to its Client, protecting the Client's vital interests, determination of appropriate therapies, making therapeutic recommendations and to be enabled to deliver expert testimony and recommendations to the Courts, legal counsel, the justice system, the social care system and Local Authorities.

4.5 Personal data held on individuals will be kept strictly private and confidential, and will not be disclosed to any third parties without permission from the individual concerned. However, personal information may be released under exemption of the Act (e.g. as requested by legal bodies in connection with criminal investigations, or if there are reasonable concerns about the risk of harm to the individual or to others).

4.6 Personal data held by the Company will:

Confidential. This document is the property of Gateway Psychology Ltd.
This is an electronic document. Paper copies may not be the latest version.

- Be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive in relation to the purpose/s for which they are processed.
- Be accurate and, where possible and necessary, kept up to date. Data obtained from third parties will be checked for accuracy where reasonable and possible.
- Not be processed for any other purpose/s
- Not be kept for longer than is necessary for that purpose/s.
- Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.
- Not transfer personal data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
- Ensure that only authorised people can access, alter, disclose or destroy personal data;
- Ensure that those people only act within the scope of their authority;
- Ensure that if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.
- Where data is held off-site (e.g. using "cloud-based" storage), the company shall satisfy itself that data is held securely and appropriately.

4.7 Personal data that is no longer needed (e.g. no longer necessary for the purposes intended), it will be disposed of in a confidential manner that will not allow recovery of the data. (e.g. shredding of paper documents or secure file deletion of computer records)

4.8 The Company will guard against loss or accidental disclosure or destruction of personal data. In particular, the Company shall:

- Design and organise the security of data to suit the nature of the personal data that we hold, anticipating the possible harm that may result from a security breach;
- Define who in is responsible for ensuring information security;
- Make sure that the Company has the right physical and technical security,
- Be ready to respond to any breach of security swiftly and effectively

4.9 The Data Protection Officer is the Business Director who will be responsible for data confidentiality and security. Periodic checks of the data security system will be conducted. The DPO is contactable at the Gateway Psychology Ltd. office.

4.10 If a breach of security results in the disclosure or loss of confidential personal data, the Company shall respond to the incident as follows:

- Implement a recovery plan, including damage limitation;
- Assess the risks associated with the breach;
- Inform the appropriate people and organisations that the breach has occurred within a 72-hour period;
- Reviewing the Company response and update the policies and procedures regarding information security.

4.11 An individual (e.g. a client) of the Company may enquire whether personal data is held by the Company and request to get copies of his/her personal data held by the Company. For traceability and record keeping purposes, this request shall be in writing. Data will be provided in a commonly used format.

4.12 In particular, an individual has

- A right of access to a copy of the information located in their personal data;
- A right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- A right to claim compensation for damages caused by a breach of the Act.

4.13 The Company shall provide the information requested to the individual within 30 days from the date of a request, unless it is exempt from providing such information by the Act.

4.14 Requests for personal data access by a child shall be provided, with consideration of the following:

- The child's level of maturity and their ability to make decisions like the data access request;
- The nature of the personal data;
- Any court orders relating to parental access or responsibility that may apply;
- Any duty of confidence owed to the child or young person;
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information;
- Any views the child or young person has on whether their parents should have access to information about them;
- Take guidance from Scottish law, where it is presumed that a child of 12 years old and older, may make requests for personal data access.

Confidential. This document is the property of Gateway Psychology Ltd.
This is an electronic document. Paper copies may not be the latest version.

4.15 If a complaint is made about the data held by the Company, it shall be dealt with via the Complaints Policy (GP-POL-001). If changes need to be made to the data stored, this shall be completed within 30 days of the complaint being upheld.

Confidential. This document is the property of Gateway Psychology Ltd.
This is an electronic document. Paper copies may not be the latest version.

5.0 CROSS REFERENCES WITH OTHER POLICIES

Complaints Policy	GP-POL-001
Safeguarding Children Policy	GP-POL-003
Health and Safety Policy	GP-POL-004

Confidential. This document is the property of Gateway Psychology Ltd.
This is an electronic document. Paper copies may not be the latest version.

CHANGE HISTORY		
Details of Change	Date of Change	Issue Level
Draft issue	13/12/2013	0
Initial Issue	22/6/2014	1
Annual review – no changes made	15/07/2015	2
Annual review – no changes made	22/05/2016	3
Revised based on GDPR requirements	27/10/2017	4
Annual review – no changes made	21/03/2018	5
Annual review, minor changes to para 4.4	31/07/2019	6
Annual review – no changes made	30/9/2021	7

Confidential. This document is the property of Gateway Psychology Ltd.
This is an electronic document. Paper copies may not be the latest version.