

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 1 of 15 Issue Level: 12

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

- Front Page - Signatories
- 1.0 Scope of policy
- 2.0 Why we need a policy
- 3.0 Key management responsibilities
- 4.0 Policy details
- 5.0 Cross references with other Gateway Psychology Policies

SIGNATORIES (signed and controlled electronically)

Dr Meryl Ann Forse

Dr M.A. Forse – Managing and Clinical Director

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 2 of 15 Issue Level: 12

1. SCOPE OF POLICY

This policy applies to all employees, workers, contracted Associates, agency workers, volunteers, trainees, service contractors and other persons who process or have access to personal, confidential or organisational information on behalf of Gateway Psychology ("Gateway").

I.1. This policy applies to information in all formats, including:

- electronic records and databases;
- clinical and assessment records;
- paper records;
- emails and electronic communications;
- photographs, audio and video recordings;
- psychometric and assessment materials;
- employee and recruitment information;
- financial and contractual information; and
- information communicated verbally.

I.2. The policy applies whether information is processed at Gateway premises, remotely, during community or home-based work, or through approved third-party, cloud or software services.

I.3. All persons covered by this policy have an individual responsibility to maintain confidentiality and comply with Gateway's data protection and information-security requirements.

2.0 PURPOSE AND FRAMEWORK

2.1 Gateway processes significant amounts of personal, confidential and special category information in providing psychological, therapeutic, assessment, consultation, training and related services.

2.2 Information processed may relate to children, young people, adults, families, employees, Associates, professionals and other individuals. It may include health and mental-health information, social-care and educational records, safeguarding information, clinical records, professional opinions and information relating to criminal offences, legal proceedings and court work.

2.3 Gateway is committed to protecting the confidentiality, integrity and availability of information entrusted to it and to respecting the privacy and information rights of individuals.

2.4 Gateway will process personal data in accordance with applicable legislation, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025; and
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where applicable.

2.5 Gateway will also have regard to:

- guidance and codes issued by the Information Commissioner's Office (ICO);
- applicable common law duties of confidentiality;
- relevant safeguarding legislation and guidance;
- Health and Care Professions Council (HCPC) standards; and
- requirements of other applicable statutory and professional bodies.

2.6 This policy should be read alongside Gateway's Privacy Notices, Record Keeping Policy, Safeguarding Policies and other relevant organisational policies and procedures.

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 3 of 15 Issue Level: 12

3.0 KEY RESPONSIBILITIES

3.1 Senior Management Team

The Senior Management Team has overall responsibility for ensuring that Gateway has appropriate governance, resources, systems and controls to comply with confidentiality, data protection and information-security requirements.

3.2 Data Protection Officer/Data Protection Lead

Gateway will designate an appropriately responsible person to oversee its data-protection arrangements.

Responsibilities include:

- advising on data-protection requirements;
- supporting compliance with this policy;
- coordinating data-subject rights requests;
- overseeing personal-data breach assessment and response;
- supporting Data Protection Impact Assessments (DPIAs);
- monitoring relevant legal and regulatory developments;
- liaising with the ICO where necessary; and
- escalating significant information-governance risks to Senior Management.

3.3 Business Director

The Business Director has responsibility for organisational IT and cyber-security oversight, including liaison with Gateway's external IT provider and oversight of Cyber Essentials arrangements.

This reflects the Cyber Essentials questionnaire, which identifies the Business Director as the person responsible internally for managing the IT systems within scope.

3.4 Practice Manager

The Practice Manager supports the day-to-day implementation of this policy, including:

- information-governance processes;
- staff training and awareness;
- user access and account administration;
- onboarding and offboarding arrangements;
- coordination with Gateway's IT provider;
- maintenance of relevant records; and
- escalation of information-security or data-protection concerns.

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 4 of 15 Issue Level: 12

3.5 Managers

Managers must ensure that staff within their areas understand and comply with applicable confidentiality, data-protection and information-security requirements.

3.6 All Staff and Associates

All staff and Associates must:

- maintain confidentiality;
- only access information they have an authorised reason to access;
- handle personal and confidential information securely;
- use only authorised systems and devices;
- comply with Gateway's access and security controls;
- complete required training;
- immediately report actual or suspected breaches, security incidents or inappropriate disclosures; and
- seek advice when uncertain about the appropriate handling or disclosure of information.

Serious or deliberate breaches may be dealt with under relevant disciplinary, contractual or professional procedures.

4.0 CONFIDENTIALITY AND DATA PROTECTION ARRANGEMENTS

4.1 Data Protection Principles

4.1.1 Gateway will process personal data in accordance with the data-protection principles.

Personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- retained for no longer than necessary;
- processed securely; and
- managed in a way which enables Gateway to demonstrate compliance.

4.1.2 Staff and Associates must only collect, access, use, share or retain personal information where this is necessary and authorised for their work.

4.2 Lawful Processing

4.2.1 Gateway will identify and document an appropriate lawful basis under Article 6 UK GDPR before processing personal data.

4.2.2 The appropriate lawful basis will depend upon the purpose and circumstances of the processing and may include contract, legal obligation, vital interests, legitimate interests or another applicable lawful basis. Current ICO guidance emphasises that the appropriate

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 5 of 15 Issue Level: 12

lawful basis must be identified before processing begins and documented; there is no single basis that is inherently preferable to another.

4.2.3 Where Gateway processes special category data, it will identify both:

- an appropriate Article 6 lawful basis; and
- an appropriate Article 9 condition for processing.

4.2.4 Special category data may include information concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- genetic data;
- biometric data used for identification;
- physical or mental health;
- sex life; and
- sexual orientation.

4.2.5 Gateway's clinical work routinely involves health information and may involve other special category information. Appropriate Article 9 conditions may therefore include provision or management of health or social care, substantial public interest, legal claims or another condition applicable to the circumstances.

4.2.6 Criminal-offence information is not treated as special category data but is subject to separate statutory protections. Gateway will only process such information where the applicable requirements are met.

4.2.7 Where the Data Protection Act 2018 requires an Appropriate Policy Document for particular processing, Gateway will maintain one.

4.3 Consent

4.3.1 Consent will not automatically be treated as Gateway's lawful basis merely because an individual has agreed to receive a service or to information being obtained.

4.3.2 Consent will only be relied upon as a data-protection lawful basis where it is appropriate and meets the legal requirements for valid consent.

4.3.3 Where consent is relied upon, it must be freely given, specific, informed and unambiguous and capable of being withdrawn.

4.3.4 Withdrawal of consent will not affect the lawfulness of processing already undertaken and does not necessarily require Gateway to cease processing where another legal requirement or lawful basis applies.

4.4 Confidentiality

4.4.1 Gateway recognises that confidentiality is fundamental to psychological practice and to the trust placed in the organisation by clients, families, commissioners and other professionals.

4.4.2 Confidential information will only be accessed, used or disclosed for an appropriate professional, organisational, contractual or legal purpose.

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 6 of 15 Issue Level: 12

- 4.4.3 Wherever appropriate, information will only be shared with those who have a legitimate need to receive it and only the minimum information necessary for the purpose will be disclosed.
- 4.4.4 Staff and Associates must not discuss confidential information where conversations may be overheard by persons who do not have a legitimate need to know.
- 4.4.5 Confidential information may sometimes be disclosed without consent, including where necessary to:
- safeguard a child or adult at risk;
 - respond to a serious risk of harm;
 - comply with a statutory obligation;
 - comply with a valid court order or other legally enforceable requirement;
 - establish, exercise or defend legal claims; or
 - meet another lawful requirement.
- 4.4.6 Where practicable, significant decisions to disclose confidential information without consent should be discussed with an appropriate senior manager, safeguarding lead, senior clinician and/or Data Protection Officer.
- 4.4.7 The rationale for significant decisions to disclose or withhold information should be appropriately recorded.

4.5 Children and Young People's Information

- 4.5.1 Gateway recognises that children and young people have their own information rights.
- 4.5.2 Information concerning children and young people will be processed fairly and transparently and with appropriate regard to their age, understanding, circumstances and vulnerability.
- 4.5.3 Where appropriate, information about Gateway's use of personal data will be provided in a format that is accessible and understandable to the child or young person.
- 4.5.4 The involvement of a parent or person with parental responsibility will depend upon the circumstances, including:
- the child's age and understanding;
 - their competence to make the relevant decision;
 - their wishes;
 - the nature and sensitivity of the information;
 - confidentiality;
 - safeguarding considerations; and
 - applicable legal requirements.
- 4.5.5 Parental responsibility does not automatically provide an unrestricted right to access all information held about a child.

4.6 Privacy Information and Transparency

- 4.6.1 Gateway will provide appropriate information about its processing of personal data through Privacy Notices and other relevant communications.
- 4.6.2 Privacy information will explain, as applicable:
- what information Gateway collects;
 - why it is collected;

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 7 of 15 Issue Level: 12

- the lawful basis for processing;
- who information may be shared with;
- retention arrangements;
- international transfers;
- individual rights; and
- how concerns or complaints may be raised.

4.6.3 Privacy information will be reviewed periodically and following material changes to Gateway's processing activities.

4.7 Information Security and Cyber Security

- 4.7.1 Gateway will maintain appropriate technical and organisational measures to protect information against unauthorised or unlawful access, processing, disclosure, alteration, destruction, damage or loss.
- 4.7.2 Gateway maintains Cyber Essentials certification across the whole organisation as part of its information-security framework. The questionnaire confirms that the certification scope covers the whole organisation rather than an isolated subset.
- 4.7.3 Gateway will maintain controls relating to the five Cyber Essentials technical areas:
- firewalls;
 - secure configuration;
 - security update management;
 - user access control; and
 - malware protection.
- 4.7.4 Gateway will maintain an appropriate inventory of devices, operating systems, significant software and cloud services.
- 4.7.5 Devices and software used to access Gateway information must be appropriately licensed, supported and maintained.
- 4.7.6 Unsupported software must be removed or appropriately managed before it presents an unacceptable security risk.
- 4.7.7 Automatic security updates will be enabled where available. High-risk and critical vulnerability fixes will be implemented within applicable Cyber Essentials timescales.
- 4.7.8 Appropriate firewall and malware protection will be maintained on Gateway devices.
- 4.7.9 Staff must not disable or circumvent Gateway security controls.
- 4.7.10 Installation of software and applications will be appropriately controlled. Staff must not install unapproved software for Gateway work.

4.8 Networks and Devices

- 4.8.1 Gateway will maintain appropriate security controls at the boundary between its organisational network and the internet and on individual devices.
- 4.8.2 Gateway maintains separate corporate and guest wireless networks. The guest network is restricted and does not provide access to Gateway's organisational information.
- 4.8.3 Gateway does not permit Bring Your Own Device (BYOD) access to organisational information or services unless specifically authorised following an appropriate information-

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 8 of 15 Issue Level: 12

security and data-protection assessment. Gateway's Cyber Essentials arrangements currently operate on a no-BYOD basis.

- 4.8.4 Gateway-issued devices must use appropriate locking mechanisms, including passwords, PINs, biometric authentication or other approved controls.
- 4.8.5 Organisational devices must be appropriately secured when unattended.
- 4.8.6 Removable media must only be used where authorised and appropriately secured.

4.9 User Accounts and Access Control

- 4.9.1 User accounts will only be created following an authorised onboarding process.
- 4.9.2 Each user will be provided with unique credentials. Shared accounts must not be used unless there is a documented and appropriately controlled technical requirement.
- 4.9.3 Access rights will be determined according to role and business requirements, applying the principle of least privilege.
- 4.9.4 Access rights must be amended where an individual's role or responsibilities change.
- 4.9.5 When an individual leaves Gateway, organisational accounts and access will be removed or disabled promptly through Gateway's offboarding process.
- 4.9.6 Gateway will periodically review user accounts and remove or disable accounts which are no longer required.

4.10 Administrator Access

- 4.10.1 Administrator privileges will be restricted to those who genuinely require them.
- 4.10.2 Administrator access must be explicitly authorised by the Business Director and/or Practice Manager and appropriately recorded. This reflects Gateway's documented Cyber Essentials arrangements.
- 4.10.3 Administrator access will be reviewed periodically and removed where it is no longer required.
- 4.10.4 Separate administrator credentials/accounts should be used for administrative activities where technically appropriate.
- 4.10.5 Administrator privileges should not routinely be used for ordinary activities such as general web browsing or email.

4.11 Authentication and Passwords

- 4.11.1 Multi-factor authentication (MFA) will be enabled for organisational cloud services where available.
- 4.11.2 MFA will be required for administrator access to cloud services where available.
- 4.11.3 Users must:
 - keep authentication credentials confidential;
 - not share passwords;
 - use passwords unique to their Gateway work accounts;
 - avoid common or readily guessable passwords; and
 - follow Gateway's current password-security requirements.

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 9 of 15 Issue Level: 12

- 4.11.4 Gateway will support secure password creation in accordance with current cyber-security guidance and technical controls.
- 4.11.5 4.11.5 Routine periodic password expiry will not be required solely because a fixed period has elapsed unless required by a particular system or security assessment.
- 4.11.6 Where a password or account is known or suspected to have been compromised, the matter must be reported immediately and the affected account secured. This may include disabling the account, changing credentials, terminating active sessions and reviewing account activity.

4.12 Remote and Home Working

- 4.12.1 Remote working may be undertaken where authorised. The same confidentiality, information-security and data-protection standards apply regardless of work location.
- 4.12.2 Gateway's Cyber Essentials scope includes regular remote workers and staff who work remotely on an ad-hoc basis.
- 4.12.3 Gateway information must only be accessed using approved devices, accounts, systems and methods.
- 4.12.4 Staff working remotely must take appropriate steps to prevent confidential information being seen, overheard or accessed by unauthorised persons.
- 4.12.5 Devices must be locked when unattended.
- 4.12.6 Confidential information must not be transferred to personal email accounts, personal cloud storage or other unapproved systems.
- 4.12.7 Device-level firewall and other security controls must remain enabled when Gateway devices are used on home or other networks.

4.13 Transporting Information

- 4.13.1 Personal and confidential information should remain within Gateway-approved electronic systems wherever reasonably practicable.
- 4.13.2 Where paper records or other confidential information must legitimately be removed from Gateway premises, they must be transported securely and protected against loss, theft or unauthorised access.
- 4.13.3 Confidential information must not be left unattended in vehicles or public places.
- 4.13.4 Information removed from Gateway premises must be returned, securely stored or securely destroyed as appropriate as soon as reasonably practicable.

4.14 Cloud Services, Software and Data Processors

- 4.14.1 Gateway uses third-party cloud and software services to support its organisational and clinical activities.
- 4.14.2 4.14.2 Gateway will maintain an appropriate record of significant cloud and third-party systems used to process organisational information.
- 4.14.3 New systems must be appropriately reviewed and authorised before they are used to process Gateway personal or confidential information.
- 4.14.4 Appropriate due diligence will be undertaken proportionate to the nature and sensitivity of the information being processed. This may consider:

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 10 of 15 Issue Level: 12

- security arrangements;
- confidentiality;
- access controls and MFA;
- processor status and contractual terms;
- sub-processors;
- data location;
- international transfers;
- retention and deletion;
- incident and breach arrangements;
- business continuity;
- backup and recovery;
- data-subject rights; and
- arrangements on termination of the service.

4.14.5 Where a supplier acts as a data processor on Gateway's behalf, an appropriate contract meeting applicable data-protection requirements will be maintained.

4.14.6 Staff and Associates must not independently introduce unapproved cloud storage, file-sharing, communication, software or online services for processing Gateway confidential or personal information.

4.15 Data Protection by Design and DPIAs

4.15.1 Gateway will consider privacy and data-protection requirements when designing or materially changing services, systems and processes.

4.15.2 A Data Protection Impact Assessment (DPIA) will be completed before processing begins where the proposed processing is likely to result in a high risk to individuals' rights and freedoms.

4.15.3 DPIA screening should be considered for significant new or changed processing involving:

- special category data;
- children or potentially vulnerable people;
- new technologies;
- systematic monitoring;
- significant data matching or profiling;
- artificial intelligence;
- large-scale processing; or
- other novel or potentially high-risk processing.

4.15.4 Identified risks and mitigating actions will be documented and addressed appropriately.

4.16 Artificial Intelligence and Emerging Technologies

4.16.1 Artificial intelligence and emerging technologies may only be used for Gateway work in accordance with Gateway's approved systems and organisational requirements.

4.16.2 Personal, confidential, clinical or special category information must not be entered into consumer or other AI systems which have not been specifically approved by Gateway to process that category of information.

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 11 of 15 Issue Level: 12

4.16.3 Before approving an AI system involving personal information, Gateway will consider as appropriate:

- purpose and necessity;
- lawful basis;
- special category conditions;
- security and confidentiality;
- supplier contractual arrangements;
- whether information is used for model training or secondary purposes;
- retention and deletion;
- international transfers;
- transparency;
- accuracy and bias;
- human oversight; and
- the requirement for a DPIA.

4.16.4 Staff remain professionally and organisationally accountable for work undertaken with AI assistance.

4.16.5 AI-generated information must be subject to appropriate human review and must not be assumed to be accurate solely because it has been generated by an AI system.

4.16.6 Gateway will not use generative AI as the sole basis for significant clinical or employment decisions concerning an individual.

4.17 Record Keeping, Retention and Disposal

4.17.1 Personal information will be retained only for as long as necessary for the purpose for which it is processed and in accordance with relevant legal, regulatory, contractual and professional requirements.

4.17.2 Specific retention arrangements will be established within Gateway's Record Keeping Policy and/or retention schedule.

4.17.3 Records must not be destroyed, altered or deleted outside authorised retention and disposal arrangements.

4.17.4 Personal and confidential information will be securely destroyed or deleted when the authorised retention period expires unless there is an appropriate reason for continued retention.

4.17.5 Paper confidential waste will be securely destroyed.

4.17.6 Electronic devices and storage media will be appropriately erased or securely disposed of before reuse, disposal or transfer where they have contained Gateway information.

4.18 International Transfers

4.18.1 Personal data will only be transferred outside the UK where permitted by applicable data-protection legislation.

4.18.2 Where required, Gateway will ensure that an appropriate international-transfer mechanism or safeguard is in place.

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 12 of 15 Issue Level: 12

4.18.3 International data transfers will be considered as part of due diligence when procuring relevant cloud, software and other third-party services.

4.19 Individual Rights

4.19.1 Individuals have rights concerning their personal information. Depending on the circumstances these may include:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights and safeguards relating to automated decision-making.

4.19.2 These rights are not absolute in every circumstance. Requests will be considered in accordance with applicable legislation and exemptions.

4.19.3 Staff receiving a request concerning an individual's information rights must promptly refer it to the Data Protection Lead.

4.20 Subject Access Requests

4.20.1 Individuals have the right to request access to their personal data.

4.20.2 A Subject Access Request (SAR) does not have to be made using a particular form or terminology and may be made verbally or in writing.

4.20.3 Staff must therefore recognise requests which may constitute a SAR and promptly forward them to the Data Protection Lead.

4.20.4 Gateway may take reasonable steps to verify the identity of a requester where necessary.

4.20.5 Gateway will respond without undue delay and normally within one month, subject to applicable provisions concerning clarification, identity verification, extensions and exemptions.

4.20.6 Gateway will undertake a reasonable and proportionate search for information falling within the scope of a request, reflecting the clarification introduced into the right-of-access framework and current ICO guidance.

4.20.7 Information relating to other individuals will be considered before disclosure and may be redacted or withheld where appropriate.

4.20.8 Particular care will be taken where requests concern clinical, health, social-care, educational, safeguarding or other sensitive records.

4.20.9 Information will be disclosed securely and in an accessible form.

4.21 Requests Concerning Children

4.21.1 Where a request concerns information about a child or young person, Gateway will consider whether they have sufficient understanding to exercise their own information rights.

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 13 of 15 Issue Level: 12

4.21.2 A parent or person with parental responsibility does not automatically have an unrestricted right to exercise the child's data-protection rights or receive all information held about them.

4.21.3 Gateway will consider, as appropriate:

- the child's age, maturity and understanding;
- the nature and sensitivity of the information;
- the child's wishes;
- the authority of a person making a request on their behalf;
- confidentiality owed to the child;
- confidentiality and rights of other people;
- safeguarding considerations; and
- applicable statutory exemptions.

4.21.4 Complex requests involving clinical, health, safeguarding, social-care or court-related information will be referred to the Data Protection Lead and, where appropriate, a senior clinician or safeguarding lead.

4.22 Personal Data Breaches and Security Incidents

4.22.1 A personal data breach includes a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include:

- information sent to the wrong recipient;
- lost records or devices;
- compromised accounts;
- cyber attacks affecting personal information;
- inappropriate disclosure;
- unauthorised access;
- accidental deletion or alteration; and
- accessing information without a legitimate reason.

4.22.2 All actual or suspected data breaches and information-security incidents must be reported immediately to the Data Protection Lead or another designated senior person

4.22.3 Staff should report concerns even where they are unsure whether an incident meets the legal definition of a personal data breach.

4.22.4 Gateway will document, investigate and risk-assess personal data breaches.

4.22.5 Where a breach is likely to result in a risk to individuals' rights and freedoms, Gateway will notify the ICO as required, without undue delay and, where feasible, within 72 hours of becoming aware of it.

4.22.6 Where a breach is likely to result in a high risk to an affected individual, Gateway will inform that individual without undue delay where required by law

4.22.7 Where an account or credential may have been compromised, Gateway will take immediate steps to secure the account and investigate potential access.

4.22.8 Lessons from breaches and near misses will be used to improve systems, controls, training and organisational practice.

4.23 Data Protection Complaints

	POLICY	No: GP-POL-006
Title: Confidentiality and Data Protection		Page 14 of 15 Issue Level: 12

- 4.23.1 Individuals may complain to Gateway about how their personal information has been handled.
- 4.23.2 Gateway will provide an accessible means of raising a data-protection complaint.
- 4.23.3 Complaints will be acknowledged, investigated and responded to in accordance with applicable data-protection requirements and Gateway's complaints arrangements.
- 4.23.4 Data-protection complaints will be referred to the Data Protection Lead.
- 4.23.5 Individuals will be informed, where applicable, of their right to complain to the ICO and seek an appropriate judicial remedy.

4.24 Training, Monitoring and Compliance

- 4.24.1 All relevant staff and Associates will receive appropriate confidentiality, data-protection and cyber-security training.
- 4.24.2 Training will be provided as part of induction and refreshed at intervals determined by Gateway's mandatory-training arrangements.
- 4.24.3 Additional training may be required following:
 - significant changes to legislation or guidance;
 - introduction of new systems or technologies;
 - identified risks;
 - data breaches or cyber incidents; or
 - identified gaps in knowledge or compliance.
- 4.24.4 Gateway will monitor its information-governance arrangements through appropriate mechanisms including:
 - training records;
 - data-breach and incident review;
 - access reviews;
 - DPIAs;
 - processor and supplier reviews;
 - data-subject requests;
 - review of organisational devices and software;
 - cyber-security arrangements; and
 - maintenance and renewal of Cyber Essentials certification.

5.0 CROSS REFERENCES WITH OTHER POLICIES

GP-POL-001 – Complaints Policy
GP-POL-002 – Equality, Diversity and Inclusion Policy
GP-POL-003 – Safeguarding Children Policy
GP-POL-004 – Health and Safety Policy
GP-POL-005 – Employment of Staff Policy
GP-POL-008 – Record Keeping Policy
GP-POL-011 – Safeguarding Vulnerable Adults Policy

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
Annual review – no changes made	17/8/2022	8
Annual review – no changes made	12/7/2023	9
Annual review – no changes made	14/9/2024	10
Annual review – updates to para 4.6	22/5/2025	11
Comprehensive annual review – policy updated to reflect current UK data protection legislation, ICO guidance and Gateway Psychology's Cyber Essentials arrangements. Sections relating to information security, data breaches, subject access, children's information, cloud services, AI and user access controls strengthened.	26/06/2026	12