PRIVACY POLICY

Behavioural Edge Psychology

Effective Date: December 2024

1. INTRODUCTION

Behavioural Edge Psychology is committed to protecting your privacy and handling your personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). This Privacy Policy explains how we collect, use, store, disclose, and manage your personal and sensitive information.

As registered psychologists with the Australian Health Practitioner Regulation Agency (AHPRA) and members of the Australian Psychological Society (APS), we also comply with the relevant codes of ethics and professional standards that govern psychological practice in Australia.

By engaging our services, you consent to the collection, use, and disclosure of your personal information as described in this Privacy Policy.

2. DEFINITIONS

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether recorded in a material form or not.

Sensitive Information: A subset of personal information that includes health information, information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal record, and membership of professional or trade associations.

Health Information: Information or an opinion about the health or disability of an individual, including information about health services provided or to be provided to that individual.

3. WHAT INFORMATION WE COLLECT

3.1 Personal Information

We may collect the following types of personal information:

- Name, date of birth, gender, and contact details (address, phone number, email)
- Medicare number and private health insurance details
- Emergency contact information
- Occupation and employment details (where relevant to treatment)
- Billing and payment information

3.2 Sensitive Information

We collect sensitive information that is necessary for providing psychological services, including:

- Health information including mental health history, diagnoses, treatment plans, and progress notes
- Information about current and past medications
- Medical history and information from other healthcare providers
- Psychological assessment results and clinical observations
- Information about family, relationships, and social circumstances
- Any other information disclosed during therapy sessions that is relevant to your treatment

4. HOW WE COLLECT INFORMATION

We collect personal and sensitive information through various means:

- Directly from you during initial intake assessments, therapy sessions, and written forms
- From your authorised representatives (with appropriate consent)
- From other healthcare providers (such as GPs, psychiatrists, or specialists) where you have provided consent
- From third parties such as insurers, Medicare, or referring professionals
- Through our website, email communications, or telephone conversations

5. WHY WE COLLECT AND USE YOUR INFORMATION

We collect and use your personal and sensitive information for the following purposes:

- To provide psychological assessment, diagnosis, treatment, and ongoing care
- To communicate with you about appointments, treatment plans, and service updates
- To process billing, insurance claims, and Medicare rebates
- To comply with legal and regulatory obligations, including AHPRA requirements
- To facilitate referrals and coordinate care with other healthcare providers (with your consent)
- For quality assurance, clinical supervision, and professional development purposes
- To respond to complaints or legal proceedings
- For de-identified research and analysis to improve our services (with appropriate safeguards)

6. RECORDING OF CLIENT SESSIONS

6.1 Audio and Video Recording

Behavioural Edge Psychology does not routinely record therapy sessions. Any audio or video recording of sessions will only occur in the following limited circumstances:

- For clinical supervision purposes where the psychologist is a provisionally registered psychologist or engaging in supervision as part of ongoing professional development
- For approved research purposes
- For specific therapeutic interventions where recording is part of the treatment approach

6.2 Consent Requirements

We will always obtain your express written consent before recording any session. You have the right to:

- Decline consent to be recorded without any impact on the quality of care you receive
- Withdraw consent at any time, including during a session
- Request that recordings be deleted after the specified purpose has been fulfilled

6.3 Storage and Security of Recordings

All recordings are:

- Stored securely on encrypted, password-protected devices
- Only accessible to the treating psychologist and their approved clinical supervisor

- Deleted within 12 months of creation unless there is a specific clinical or legal reason for retention
- Subject to the same confidentiality protections as written clinical records

6.4 Client-Initiated Recordings

Clients are not permitted to record therapy sessions without the express written consent of the psychologist. Unauthorized recording of sessions may result in termination of the therapeutic relationship.

7. HOW WE STORE AND SECURE YOUR INFORMATION

7.1 Security Measures

We implement comprehensive security measures to protect your information:

- Electronic records are stored on secure, encrypted servers with restricted access
- Paper records are stored in locked filing cabinets within secure premises
- All staff and contractors are bound by confidentiality agreements
- Access to client information is restricted to authorised personnel on a need-to-know basis
- Regular security audits and updates to protect against unauthorized access
- Secure communication channels for transmission of sensitive information

7.2 Retention of Information

Retention Periods:

In accordance with AHPRA guidelines and professional standards, we retain client records for the following minimum periods:

- Adult clients: 7 years from the date of the last service or contact
- Clients who were minors at the time of service: 7 years from the date the client turned 18 years of age, or 7 years from the date of the last service, whichever is later
- Records relating to legal proceedings or complaints: Until the matter is fully resolved plus 7 years

Purpose of Retention:

We retain your information to:

- Ensure continuity of care if you return for future treatment
- Comply with legal and professional obligations
- Respond to complaints or legal proceedings
- Support clinical supervision and quality assurance processes

7.3 Destruction of Information

After the required retention period, records are securely destroyed through: (a) shredding and secure disposal of paper records; (b) permanent deletion and overwriting of electronic records; and (c) destruction of any backup copies. Destruction is documented and logged in accordance with our record management procedures.

8. DISCLOSURE OF INFORMATION

8.1 Disclosure with Consent

With your written consent, we may disclose your information to:

- Your general practitioner or other treating healthcare providers
- Private health insurers for the purpose of processing claims
- Medicare and the Department of Human Services for rebate processing
- Referring professionals or organizations
- Family members or support persons you have nominated

8.2 Disclosure Without Consent

We may disclose your information without your consent where:

- Required or authorized by law (e.g., court orders, subpoenas, or mandatory reporting obligations)
- Necessary to prevent or lessen a serious threat to your life, health, or safety, or that of another person or the public
- Required for child protection reporting obligations under state and territory legislation
- Necessary to investigate or respond to suspected unlawful activity or serious misconduct
- Required to comply with AHPRA investigations or professional conduct proceedings

8.3 Clinical Supervision and Professional Development

Your information may be discussed in clinical supervision or peer consultation for quality assurance and professional development purposes. In such cases, we take reasonable steps to de-identify information where possible, and all supervisors and colleagues are bound by the same confidentiality obligations.

9. NOTIFIABLE DATA BREACHES

9.1 The Notifiable Data Breaches Scheme

Under the Privacy Act 1988 (Cth), Behavioural Edge Psychology is subject to the Notifiable Data Breaches (NDB) scheme. This scheme requires us to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to individuals.

9.2 What is an Eligible Data Breach

An eligible data breach occurs when:

- There is unauthorized access to, unauthorized disclosure of, or loss of personal information that we hold
- This is likely to result in serious harm to one or more individuals

Examples of eligible data breaches may include theft of devices containing unencrypted client information, ransomware attacks that compromise client data, unauthorized access to client files by staff or third parties, or accidental disclosure of client information to the wrong recipient.

9.3 Assessment of Data Breaches

When we become aware of a suspected data breach, we will conduct an immediate assessment to determine whether it is an eligible data breach. This assessment will be

completed as soon as practicable, and within 30 days of becoming aware of the suspected breach.

Our assessment process includes:

- Identifying what personal information has been involved
- Determining how the breach occurred
- Assessing the risk of serious harm to affected individuals
- Considering whether remedial action can prevent serious harm from occurring

9.4 Notification Requirements

If we determine that an eligible data breach has occurred, we will:

1. Notify the OAIC as soon as practicable using the approved form
2. Notify affected individuals directly (or, if that is not practicable, publish a statement on our website)

The notification will include:

- A description of the data breach
- The kind of information concerned
- Recommendations about steps you should take in response to the breach
- Contact details for further information

9.5 Our Response and Remediation

In the event of a data breach, we will:

- Take immediate action to contain the breach and prevent further unauthorized access or disclosure
- Conduct a thorough investigation to understand the cause and extent of the breach
- Implement remedial measures to prevent similar breaches in the future
- Provide support and assistance to affected individuals
- Review and update our security practices and policies as necessary

9.6 Reporting a Suspected Breach

If you suspect that your personal information has been compromised or accessed without authorization, please contact us immediately using the details provided in Section 15 of this policy.

10. YOUR RIGHTS AND CHOICES

10.1 Access to Your Information

You have the right to request access to the personal information we hold about you. To request access, please contact us in writing using the details in Section 15. We will respond to your request within 30 days.

We may charge a reasonable fee to cover the administrative costs of providing access to your records. We will inform you of any fees before processing your request.

In certain circumstances, we may deny access to your information, such as where providing access would pose a serious threat to the life, health, or safety of any individual, or where it would have an unreasonable impact on the privacy of others. If we deny access, we will provide you with written reasons for the denial.

10.2 Correction of Information

You have the right to request correction of personal information we hold about you if you believe it is inaccurate, out-of-date, incomplete, irrelevant, or misleading. We will take reasonable steps to correct the information and will respond to your request within 30 days.

If we disagree with your requested correction, we will provide you with written reasons and you may request that we attach a statement to your record noting that you dispute the accuracy of the information.

10.3 Withdrawal of Consent

You may withdraw your consent to the collection, use, or disclosure of your information at any time, subject to legal and contractual restrictions. However, withdrawing consent may affect our ability to provide services to you.

11. THIRD PARTY SERVICE PROVIDERS

We may engage third party service providers to assist with:

- Electronic health record management and practice management software
- Secure data storage and backup services
- Professional indemnity insurance
- Accounting and financial services
- IT support and cybersecurity services

All third-party service providers are required to comply with the APPs and are bound by confidentiality obligations. We conduct due diligence to ensure that third parties have appropriate security measures in place to protect your information.

12. OVERSEAS DISCLOSURE

We generally do not disclose personal information to overseas recipients. However, some of our third-party service providers (such as cloud storage providers) may store data on servers located outside Australia.

Where we use service providers that store data overseas, we take reasonable steps to ensure they comply with the APPs or are subject to similar privacy protections. Countries where data may be stored include the United States and countries within the European Union. We will notify you if circumstances change such that your information will be disclosed to overseas recipients.

13. WEBSITE AND ONLINE PRIVACY

Our website may collect certain information automatically, such as IP addresses, browser types, and pages visited. This information is used for website administration and improvement purposes only.

We use cookies and similar technologies to enhance user experience. You can configure your browser to reject cookies, but this may affect website functionality.

Any information you submit through our website contact forms or appointment booking system is transmitted securely and handled in accordance with this Privacy Policy.

14. COMPLAINTS AND CONCERNS

If you have a complaint about how we have handled your personal information, please contact us in writing using the details in Section 15. We will:

- Acknowledge your complaint within 7 days
- Investigate your complaint thoroughly and impartially
- Provide a written response within 30 days outlining our findings and any action taken

If you are not satisfied with our response, you may lodge a complaint with:

Office of the Australian Information Commissioner (OAIC)

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Website: www.oaic.gov.au

You may also lodge a complaint with the Australian Health Practitioner Regulation Agency (AHPRA) at www.ahpra.gov.au if you believe there has been a breach of professional standards.

15. CONTACT INFORMATION

If you have any questions about this Privacy Policy or wish to exercise your rights, please contact us:

Behavioural Edge Psychology

Privacy Officer

[Insert Physical Address]

Phone: [Insert Phone Number]

Email: privacy@behaviouraledgepsychology.com.au

16. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or for other operational reasons. The current version will always be available on our website and at our practice.

We will notify current clients of any material changes to this policy that may affect how we handle their personal information. Notification may be provided via email, during appointments, or through a notice on our website.

Your continued use of our services following any changes to this Privacy Policy will constitute your acceptance of such changes.