Client Privacy Notice

Counselling With Keith
TOWARDS HEALING THROUGH CONNECTION

I take the privacy, including the security, of the Personal Information I hold about you seriously. This privacy notice tells you how I collect Personal Information about you and how I hold, use, and protect that Personal Information in compliance with the **UK GDPR** and **Data Protection Act 2018**. You should read this privacy notice carefully so that you know and can understand why and how I use the Personal Information I collect and hold about you.

It is important that you **keep your Personal Information up to date**. If any of your Personal Information changes, please contact me as soon as possible to let me know. If you do not contact me to keep your information updated, it may prevent me from providing the services you have requested.

1. Data Controller Contact Information

I am **Keith Johnston**, a counsellor based in **Coleraine, Northern Ireland**. I am the Data Controller of the personal information I collect, hold and use about you, as explained in this notice.

If you have any questions about how I handle your personal information, or if you wish to exercise any rights under data protection law, please contact me at:

- **Telephone:** 07359 082 687
- **Email**: email@counsellingwithkeith.com

2. Key definitions

The key terms used in this privacy notice are defined below, for ease:

- **Data Controller**: the organisation or person responsible for deciding how Personal Information is collected, stored, and used.
- **Data Processor**: a Data Controller may appoint another organisation or person to carry out certain tasks on its behalf in relation to the Personal Information.
- **Personal Information / Data**: any information from which a living individual can be identified. It does not apply to information that has been anonymised.
- **Special Category Data**: certain very sensitive Personal Information requires extra protection under data protection law. Sensitive data includes information relating to health, racial and ethnic origin, political opinions, religious and similar beliefs, trade union membership, sex life, and sexual orientation. It also includes genetic information and biometric information.

3. What Personal Information I Collect

I collect personal information directly from you, typically via a **client details form**, and through subsequent **communication** or **counselling sessions**. The information I collect can include:

- **Personal Details**: Full name, address, date of birth/age, telephone number, and email address.
- **Emergency Contact Details**: GP contact information. Details of an emergency contact and their relationship to you.
- **Current Medication**: Details of medications you are taking (if you choose to disclose).
- **Mental Health and Well-being:**
  - Current mental health concerns, presenting challenges, issues, or ongoing stressors.
  - Current mood and emotional state.
  - Relevant family history, personal history or lifestyle factors potentially affecting mental health.
  - Any risks or safety concerns (including self-harm, suicide risks, or other factors impacting your welfare).
  - Previous counselling experiences, and any other healthcare professionals currently supporting you.
- **Social & Family Context**: Information about your living arrangements, personal relationships and support networks. Your daily routines or activities including hobbies or interests that may inform your well-being.
- **Session Records**: Brief notes recorded after each session to capture key topics, observations, mental or emotional states, and any risk-related concerns you share. Worksheets, images, or additional notes created or used during sessions to facilitate therapeutic work.
- **Communications**: Any written or digital communications exchanged between us, including letters, emails, text messages, or call logs.
- **Scheduling & Attendance Records**: Times and dates of booked appointments, any cancellations or rescheduling, and related attendance information.
- **Additional Information**: Topics or issues you'd like to address in counselling, your goals or expectations for counselling, other details that may affect your well-being, and any accommodations required to ensure your comfort or safety.

Some of the information I collect is considered **special category data** under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. I collect and hold the following types of special category data about you:

- Health

I **may** hold the following special category data **if provided by you**:

- Race
- Ethic origin
- Politics
- Religion
- Sex life
- Sexual orientation

I **do not** collect information from you relating to criminal convictions or offences.

I process this data to provide healthcare (counselling) services responsibly and lawfully, in line with **Article 9(2)(h)**.

4. Why I Collect Your Personal Data

4.1. Purpose of Collection

- **Provide Appropriate Counselling Services** To tailor our sessions and interventions to your specific needs, considering personal and family history, mental health status, and any relevant social or lifestyle factors that may influence your well-being.
- **Manage Communication & Administration** To schedule appointments, confirm attendance, handle cancellations, and maintain clear channels of communication (e.g., via email or text messages).
- **Keep Accurate Session Records** To document the key themes, observations, risks, and notable changes from each counselling session (e.g., keeping brief notes, worksheets, images). These notes help me deliver effective support, to ensure continuity of care and to adhere to professional standards and insurance obligations.
- **Assess Risk & Ensure Safety** To identify and respond to potential risks affecting your welfare (e.g., self-harm or suicidal ideation). In urgent situations, I may contact your GP, emergency contact, or emergency services if necessary for your safety or the safety of others.
- **Accommodate Individual Needs** To consider a range of personal circumstances or differences that may affect how you

process, communicate, or engage with therapy, and to make adjustments that ensure sessions remain accessible, supportive, and beneficial to you.

4.2. Lawful Bases for Processing

Under UK GDPR, I must have a lawful basis for processing your personal data. I rely on the following lawful bases:

- **Consent,** in accordance with **Article 6(1)(a)**: Where you voluntarily provide specific information (e.g., details of current medication) or agree to certain processes (such as sharing risk-related data with relevant parties).
- **Contract**, in accordance with **Article 6(1)(b)**: To fulfil the counselling services you have requested, which includes scheduling and managing your appointments, providing counselling sessions, and communicating essential session details.
- **Legal Obligation**, in accordance with **Article 6(1)(c)**: To comply with legal obligations that apply to my counselling practice. This includes disclosing information when **required by law**, such as court orders or statutory **duties related to safeguarding** and the **prevention of harm**.
- **Vital Interests**, in accordance with **Article 6(1)(d)**: In rare circumstances, to protect your life or someone else's if there is a serious, imminent risk to safety.
- **Legitimate Interests**, in accordance with **Article 6(1)(f)**: For essential practice operations supporting the provision of services such as maintaining records, protecting IT systems, and ensuring the overall efficiency of the counselling service, provided these interests do not override your fundamental rights or freedoms.

For some of the purposes, I may have **more than one legal basis** on which I use your personal data, because the legal basis may be different in different circumstances.

Where I hold **special category data** I usually do so under the legal bases of consent, necessity for the provision of mental health services, contract, or, in limited emergency circumstances, vital interest.

5. How I Use Your Information

- **Counselling Sessions**: Your data helps me tailor my therapeutic approach to support your emotional well-being and mental health.
- **Session Records**: I keep brief session notes and other relevant information to deliver effective support and ensure continuity of care.
- **Safety & Emergencies**: If I have serious concerns about your safety or someone else's, I may use your emergency contact or GP details to seek extra support.
- **Communication**: I use your contact details to schedule appointments, provide updates, or respond to your queries.

6. Sharing Your Information

- **Professional Supervision**: As is standard in counselling practice, in my professional supervision I may discuss clinical material in an anonymized manner to ensure effective and ethical practice. No personally identifiable data is shared.
- **Healthcare Professionals, Emergency Services or Emergency Contact**: If needed to protect your vital interests (e.g., imminent risk of harm), I may share limited information with your GP, your emergency contact, a hospital, or the emergency services. While I routinely collect Emergency Contact information as a precautionary measure, I only use or share this information in actual emergencies.
- **Professional or Legal Requirements**: Confidential information may be disclosed when required by law (e.g., a court order), or relevant professional membership bodies, including situations where it is necessary to respond to formal inquiries or legal claims.
- **Third-Party Services and Data Processors**: See Section 10 for information on how your data is processed and stored by trusted third parties.
- **Clinical Will**: In the unforeseen event that I become seriously incapacitated, die, I have appointed a trusted professional colleague as my Clinical Executor. This colleague is a qualified practitioner bound by the same ethical and legal standards of confidentiality and data protection under the GDPR. The Clinical Executor will have limited access to your contact information solely for the purpose of informing you of the situation and discussing suitable arrangements for your continued care, such as referrals to another qualified therapist. No therapeutic content or sensitive personal data will be disclosed.

I do not sell or trade your personal data to any third parties.

7. Data Retention

I retain your personal data for **7 years** following the end of our counselling relationship, in line with professional guidelines, insurance requirements, and legal considerations. After that period, I will **securely destroy** or **permanently anonymize** your data.

8. Your Rights

Under UK GDPR, you have the following rights regarding your personal data:

- **Right to Be Informed**: You have the right to clear, transparent, and easily understandable information about how I use your data (this Privacy Notice fulfils that right).
- **Right to Request Access**: Also known as "subject access". You can request a copy of the personal data I hold about you and information on how I process it.
- **Right to Correction**: You have the right to request that any incorrect personal data is corrected, and that any incomplete personal data is completed.
- **Right to Erasure (Where Applicable):** You may be entitled to have your data erased. Where I rely on consent as the legal reason for processing your personal data for a specific purpose, you have the right under data protection law to withdraw your consent at any time. If I receive a request from you withdrawing your consent to a specific purpose, I will stop processing your personal data for that purpose, unless I have another legal reason for processing your personal data – in which case, I will confirm that reason to you. I may need to keep certain records for insurance requirements, professional requirements, or legal considerations.
- **Right to Restrict Processing**: In certain circumstances, you can ask me to limit how your data is used.
- **Right to Data Portability**: this right allows you to request that I transfer your personal data to someone else.
- **Right to Object**: You may object to certain types of processing that rely on Legitimate Interests. If I can demonstrate compelling grounds for processing or if processing is otherwise required by law, your objection may not override these grounds.

Where I rely on consent as the legal basis for using your personal data, you have the **right to withdraw your consent**.

To exercise any of these rights, please contact me using the contact details in **Section 1**. I will respond as quickly and comprehensively as possible, in accordance with my professional and legal obligations.

I may need certain information from you so that I can verify your identity. I do not charge a fee for exercising your rights unless your request is unfounded or excessive. If your request is unfounded or excessive, then I may refuse to deal with your request.

9. Data Storage, Security Measures and Encryption

I take reasonable and appropriate steps to protect your data against unauthorized access, loss, or misuse. Accordingly, I use multiple layers of protection to safeguard your information.

9.1. Online Form Encryption

- I use Jotform's Encrypted Forms to collect new client details via **end-to-end encryption (E2EE)**. This means form data is encrypted on the client's device and remains encrypted in transit to Jotform and while stored by Jotform at rest. The data can **only** be decrypted (unlocked) by me with my access code.
- As a result of this **end-to-end encryption (E2EE), no one** — including Jotform — can view your personal data without possessing my account password and access code.
- Once received from Jotform, I move your data into a **secure, local password-protected system**.

9.2. Local Data Storage & Encryption

- **Encrypted Local Data Storage**: All local data—except for data stored on a mobile phone—is securely stored using **AES-256 encryption**, a widely recognized industry standard. The data remains encrypted when not in active use ensuring it cannot be accessed without a valid encryption key.
- **Data Stored on Mobile Phone**: To facilitate communication between us, your initials, phone number, appointment times, our call logs, and text messages may be stored on a mobile phone **without additional encryption**. Access to the mobile phone is secured with **biometric authentication** (fingerprint recognition) or a **strong passcode** to prevent unauthorized access.
- **Emails on Mobile Phone**: Emails you send to me may also be stored on my mobile phone. These emails are stored in an **encrypted** format managed by the Email Service Provider's app (see Section 10.3). The app can only be accessed and the data decrypted using **biometric authentication** or a **strong passcode** on the device.

9.3. Secure Cloud Backup

- I maintain **offsite encrypted backups** using a cloud backup service, ensuring that no single event (e.g., hardware failure, local disaster) will cause the permanent loss of your data.
- The data is **end-to-end encrypted (E2EE)**, ensuring that **your data remains protected**. The data is encrypted *before* it ever leaves my local system, is encrypted during transfer and remains encrypted on the cloud backup storage.
- The encryption key is **never shared** with the cloud storage provider, which means they have absolutely no access to the data. Only I can decrypt and view the information.

9.4. Physical Notes

- In the rare event I keep physical notes or printed records, these documents are stored in locked cabinets or drawers. Access is strictly limited to me.

With these measures in place, no third party can access your decrypted data. I regularly review these security practices to ensure they meet or exceed data protection requirements.

10. Third-Party Services and Data Protection

I use trusted third-party data processors to facilitate my services. When these services involve processing your Personal Data, I ensure that appropriate legal and security arrangements are in place to protect your information, in line with UK GDPR.

- Where a third party acts as a **Data Processor** on my behalf, I will have a formal Data Processing Agreement (DPA) in place. This contract outlines their responsibilities and obligations, including in respect of the security of Personal Information.
- Where a third-party service provider acts as a **Data Controller** for the services they provide, I undertake due diligence to ensure they have robust data protection measures, meet their own legal obligations under data protection law, and have appropriate safeguards (such as Standard Contractual Clauses for international transfers, where applicable) before I use their services.

The specific role of each third party (as Data Processor or Data Controller) and the nature of my arrangement with them are further clarified in the sections below. Third parties include but are not limited to:

10.1. Online Form Hosting & eSignatures

- **Service Provider:** Jotform Ltd. (UK/EU) & Jotform Inc. (US) ("Jotform").
- **Addresses:**
  - Jotform Ltd., 25 Cabot Square, London E14 4QZ
  - Jotform Inc., 4 Embarcadero Center, Suite 780, San Francisco CA 94111
- **Use:** To collect form submissions and electronic signatures.
- **Role:** As Data Processor, storing this data and only processing it in ways I instruct.
- **Security:** Form submissions are end-to-end encrypted (E2EE), meaning your form data is encrypted at every stage. Neither Jotform nor any third party can decrypt your submissions unless they have my private access code.
  For eSignatures, your name, email address and IP address are processed by Jotform.
- **Compliance**: GDPR compliant, Data Processing Addendum (DPA) in place.
- **International Data Transfers:** Jotform may process data on servers located outside of the UK or EEA. However, Jotform has put in place appropriate safeguards—such as Standard Contractual Clauses (SCCs) or the UK Addendum—to ensure your data remains protected.
- **Policies**:
  - Jotform Privacy Policy: https://www.jotform.com/privacy/
  - Jotform GDPR Compliance: http://jotform.com/gdpr-compliance/

10.2. Secure Cloud Backup

- **Service Provider:** Dropbox International Unlimited Company ("Dropbox").
- **Address:**
  - One Park Place, Hatch Street Upper, Dublin 2, D02 FD79.
- **Use:** Offsite backup of locally encrypted data.
- **Role:** As Data Controller of encrypted data. Dropbox states that it acts as a Data Controller regarding data stored in their system.

Despite this classification, I remain the primary Data Controller under GDPR for the data I gather and upload while providing my counselling services.

- **Security:** Data is securely transferred to Dropbox using a secure communication protocol (SSL/TLS). Dropbox then encrypts and stores this data on its servers using 256-bit Advanced Encryption Standard (AES). This is an additional layer of encryption on top of the local encryption I apply.
- **Compliance**: GDPR compliant. Even though Dropbox considers itself a Data Controller for my account, I monitor and remain responsible for how your data is collected, retained, and deleted (i.e., I am the primary Data Controller under GDPR). Dropbox has robust security and privacy commitments, as outlined in their Shared Responsibility Guide (linked below). If Dropbox changes its practices significantly, I will reassess its suitability and ensure your data remains protected.
- **International Data Transfers:** Dropbox may process data on servers located outside of the UK or EEA. However, Dropbox has put in place appropriate safeguards — such as Standard Contractual Clauses (SCCs), the EU-US Data Privacy Framework or the UK Addendum — to ensure your data remains protected.
- **Policies**:
  - Dropbox Privacy Policy: https://www.dropbox.com/privacy
  - Dropbox GDPR Compliance: https://www.dropbox.com/en_GB/security/gdpr
  - Dropbox Shared Responsibility Guide: https://assets.dropbox.com/documents/en/trust/shared-responsibility-guide.pdf

10.3. Email, Secure Email & Calendar

- **Service Provider:** Proton AG, Proton Europe sàrl (EU Representative) ("ProtonMail").
- **Addresses:**
  - Proton AG, Route de la Galaise 32, 1228 Plan-les-Ouates, Switzerland.
  - Proton Europe sàrl, rue de Grünewald 94, L-1912 Luxembourg.
- **Use:** I use ProtonMail for sending and receiving standard and secure emails and managing a secure calendar.
- **Role:** GDPR Compliant. Under GDPR, ProtonMail primarily acts as a Data Controller for its service operation and infrastructure. However, I remain responsible for any personal data I store or transmit via ProtonMail in the course of my counselling practice.
- **Security:**
  - ProtonMail employs zero-access end-to-end encryption (E2EE) where possible. Messages sent between ProtonMail accounts are encrypted automatically. Emails to non-Protonmail addresses are secured via SSL/TLS in transit but may not be fully encrypted on the recipient side.
  - ProtonMail offers a Secure Email service where the email will be encrypted on ProtonMail's servers and the recipient receives a standard email with the link to view the secure email which can only be decrypted and accessed by the recipient with the correct password.
  - To operate all email services ProtonMail must have access to sender and recipient email addresses, the IP address incoming messages originated from, attachment name, message subject, and message sent and received times. They do not have access to secure email message content.
  - Calendar events are similarly protected by Proton encryption protocols, though metadata (e.g., organizers' names, times) may be processed by Proton's servers.
  - I ensure strong passwords and carefully manage device and account access.
- **Compliance**: ProtonMail operates under Swiss and GDPR-aligned privacy regulations. They have robust technical and organizational measures in place. ProtonMail is not engaged strictly as a Data Processor on my behalf. Nonetheless, I remain compliant by having technical safeguards and ensuring data subject rights and data protection principles are upheld.
- **International Data Transfers**: ProtonMail's servers are predominantly located in Switzerland, but encrypted data may traverse networks outside of the UK/EEA. Proton commits to GDPR-level protection, with any necessary transfer safeguards in place.
- **Policies**:
  - ProtonMail Privacy Policy: https://proton.me/legal/privacy
  - ProtonMail GDPR Overview: https://proton.me/support/is-proton-mail-gdpr-compliant

11. Updates to This Privacy Notice

I may **periodically update** this Privacy Notice to reflect any changes in my practice or in professional or legal obligations.

Data processors may be added or changed but will always ensure **equivalent or stronger protections** are in place. For an up-to-date list of processors, please check this Privacy Notice periodically.

When I make significant updates that materially affects your privacy rights or how your data is processed, I will **notify current clients directly** (e.g., by email or during a session) and provide the revised notice. Previous clients may find **revised notices online** at https://www.counsellingwithkeith.com/privacy

12. Questions or Concerns?

If you have any questions about this Privacy Notice or how I handle your data, please contact me at:

- **Telephone:** 07359 082 687
- **Email**: email@counsellingwithkeith.com

You can view **The UK General Data Protection Regulation (UK GDPR)** at:
https://www.legislation.gov.uk/eur/2016/679/contents

You can view **The Data Protection Act 2018** at:
https://www.legislation.gov.uk/ukpga/2018/12/contents

For further details on data protection and your rights, you may also consult:
The **Information Commissioner's Office (ICO)** at https://ico.org.uk/ or by calling 0303 123 1113.

For the **latest version of this privacy notice** or alternative formats, please visit:

https://www.counsellingwithkeith.com/privacy