Data Breach Policy

1. Introduction

PsyConnect is committed to ensuring the confidentiality, integrity, and availability of personal data. In the event of a data breach, this policy provides a structured approach to respond effectively, mitigate harm, and comply with legal obligations, such as the General Data Protection Regulation (GDPR).

2. Objectives

The objectives of this policy are:

- To minimise the impact of data breaches on affected individuals and the organisation.
- To ensure compliance with regulatory requirements, including timely notification to relevant authorities and affected individuals.
- To prevent future breaches by identifying and addressing root causes.

3. Scope

This policy applies to:

- All personal data processed by PsyConnect, including data from clients and therapists.

- Therapist Professional information not available in the public domain.
- All systems, platforms, and third-party services used to store or process data.

4. Definition of a Data Breach

A data breach refers to any incident leading to:

- Unauthorised access to personal data.
- Loss or theft of personal data.
- Unintentional disclosure of personal data.
- Alteration or destruction of personal data without proper authorisation.

Examples include hacking incidents, lost devices containing data, accidental email disclosures, or ransomware attacks.

5. Responsibilities

- **Ruth and Francisco Flores**: As the sole administrators, they are responsible for detecting, managing, and resolving data breaches.
- **Third-Party Providers (e.g., Wix)**: Responsible for maintaining secure systems and promptly notifying PsyConnect of any platform-related breaches.

6. Breach Management Process

PsyConnect follows a four-phase approach to manage data breaches effectively:

6.1. Detection and Reporting

- Breaches are detected through:
    - Wix's 24/7 monitoring systems, which alert administrators of anomalies.
    - Reports from users, third parties, or external systems.
- Any suspected breach should be reported immediately to admin@psyconnect.co.uk

6.2. Containment and Assessment

- Ruth and Francisco will immediately:

    - Contain the breach to prevent further unauthorised access or damage.
    - Secure affected systems and isolate compromised data.
    - Collaborate with Wix or other third-party providers for forensic analysis if needed.
- Assess the breach to determine:
    - The type and sensitivity of the data involved.
    - The extent of the breach, including the number of affected individuals.
    - Potential risks to individuals, such as identity theft, financial loss, or privacy violations.

6.3. Notification

If the breach poses a risk to individuals' rights and freedoms:

- **Regulatory Authorities**:
    - Notify the Information Commissioner's Office (ICO) or relevant authority within 72 hours of becoming aware of the breach.
    - Provide the following details:
        - Nature of the breach (e.g., type of data involved, scope).
        - Likely consequences of the breach.
        - Measures taken or proposed to address the breach.
- **Affected Individuals**:
    - Notify affected users promptly if the breach is likely to result in significant harm.
    - Provide clear information, including:
        - The nature of the breach and its potential impact.
        - Steps they should take to protect themselves (e.g., changing passwords).
        - Contact information for further assistance.

6.4. Recovery and Follow-Up

- Restore normal operations by addressing vulnerabilities and implementing stronger controls.
- Conduct a post-breach review to:

    - Identify root causes and recommend improvements to policies, procedures, or technical safeguards.
    - Document the incident, response, and lessons learned.

7. Record-Keeping

- PsyConnect will maintain a Breach Register to log:
    - Details of any breach (e.g., date, type of data involved).
    - Actions taken to contain and mitigate the breach.
    - Communication with authorities and affected individuals.
    - Recommendations to prevent future breaches.
- The Breach Register table is created and is a tab of the PsyConnect Information Asset Register and Record of Processing Activity document.

8. Preventive Measures

To reduce the likelihood of data breaches, we:

- Use robust security measures, including encryption, access controls, and secure authentication.
- Maintain an active Information Asset Register (IAR), Record of Processing Activities (ROPA), and Data Protection Impact Assessment (DPIA).
- Utilise antivirus software with firewalls to protect against malware and unauthorised access.
- Install updates to Windows and other devices promptly when available to ensure up-to-date security.
- Implement anti-spam and CAPTCHA technology to prevent automated attacks and spam submissions.
- Have feedback and complaints procedures to identify and address security concerns effectively.

9. Third-Party Provider Collaboration

- Ensure that third-party providers, such as Wix, comply with stringent security requirements.

- Require immediate notification from providers if their systems are compromised and involve shared data.

10. Policy Review

This policy will be reviewed annually or after any significant data breach to ensure it remains effective and up-to-date with regulatory requirements and best practices.

11. Contact Information

To report a suspected data breach or for further information, contact:

- **Email**:admin@psyconnect.co.uk
- **Phone**: 07735082994

Updated: 9 December 2024