PATHWAYPIXEL

GAMING WITH PURPOSE, EMPOWERING NEURODIVERSE JOURNEYS

Cybersecurity Policy

1. Introduction

At PathwayPixel, we prioritize the security of our clients' data, including their personal and sensitive information, during all online interactions. As part of our commitment to safeguarding data, this policy outlines the measures we take to ensure the security and integrity of all digital systems used in our gaming mentorship sessions.

2. Data Security Practices

We use secure systems and platforms to conduct our gaming sessions and store client data. All sensitive information is protected through a combination of physical, administrative, and technical safeguards. The following measures are in place:

- **Encryption**: All personal data, including client details, session recordings, and communication, is encrypted to ensure protection from unauthorized access.
- **Secure Platforms**: We use reputable platforms like **Discord** for communication and **Google Workspace** for storing reports and documents. These platforms comply with GDPR and industry best practices for data security.
- **Access Control**: Only authorized staff members have access to client data. Access is limited based on job roles, and staff accounts are regularly reviewed and updated to ensure compliance with our security standards.

3. Password Management

To protect all accounts, we follow strict password policies:

- **Strong Passwords**: Staff and clients are required to use strong, unique passwords for any accounts related to their sessions (e.g., Discord, Google Workspace). Passwords must include a combination of letters, numbers, and special characters.
- **Two-Factor Authentication (2FA)**: All staff accounts are protected with two-factor authentication where possible. We encourage clients and parents to enable 2FA for their accounts to add an extra layer of security.

4. User Access Control

We implement the following user access protocols to ensure that client data is accessible only to those who need it:

- **Role-Based Access**: Staff are assigned specific access rights based on their roles. For example, session coordinators will have access to session data, but not to sensitive client information unless necessary.

- **Client Access**: Clients will have access only to their own data and session materials. They will not be able to access other clients' information or sessions.

5. Session Monitoring and Security

To ensure the safety of all gaming sessions, we monitor interactions in real time. Our monitoring protocols include:

- **In-Session Monitoring**: All gaming sessions are monitored for security and safety purposes to prevent bullying, harassment, or inappropriate content.
- **Recording for Safety**: Some sessions may be recorded, with prior consent, for training and safety monitoring purposes. Clients and parents will be notified in advance if a session is recorded.

6. Incident Response and Data Breach Procedures

In the event of a cybersecurity breach or data loss, we follow a strict protocol:

- **Immediate Action**: If a data breach is detected, our response team will immediately isolate the compromised systems to prevent further damage.
- **Notification**: We will notify affected clients within 72 hours of identifying the breach, as required by GDPR. Clients will be informed of the nature of the breach and what steps are being taken to mitigate the damage.
- **Investigation**: A full investigation will be conducted to determine the cause of the breach, and necessary measures will be taken to prevent future occurrences.

7. Data Backups

We perform regular backups of all critical data to ensure continuity and recovery in case of an incident. Backups are securely stored and are only accessible to authorized personnel.

8. Staff Training

All staff members undergo regular training on cybersecurity best practices, including:

- Identifying phishing attacks and other security threats.
- Proper handling and storage of sensitive client data.
- How to report potential security incidents.

9. Secure Communication Channels

To ensure all communication during sessions is secure:

- **Voice and Video Sessions**: All sessions held via platforms like Discord are conducted using secure, encrypted channels. We recommend that both clients and staff use private accounts to minimize exposure to security threats.
- **Messaging**: Any direct messages exchanged during sessions will be conducted through encrypted messaging services (e.g., Discord).

10. Compliance with Laws and Regulations

We comply with all relevant data protection laws, including **GDPR**, to ensure the highest standards of data protection. We also comply with applicable cybersecurity regulations to ensure the security of our digital infrastructure.

11. Third-Party Security
We work only with third-party service providers (such as Discord, Google Workspace, etc.) that have demonstrated compliance with data protection regulations and industry standards for cybersecurity.