Policy Framework for Compliance with AI Ethics Principles

1. Human, Social, and Environmental Wellbeing

- **Policy**: All AI systems developed or implemented by the business must prioritize human, social, and environmental wellbeing. This includes ensuring that AI applications enhance the quality of life for employees, customers, and the community, without causing harm to the environment or society.
- **Implementation**:
    - Conduct impact assessments to evaluate the social and environmental effects of AI projects.
    - Prioritize AI use cases that contribute positively to social wellbeing, such as improving workplace safety, health outcomes, or environmental sustainability.
    - Regularly review and adjust AI systems to ensure they align with corporate social responsibility goals.

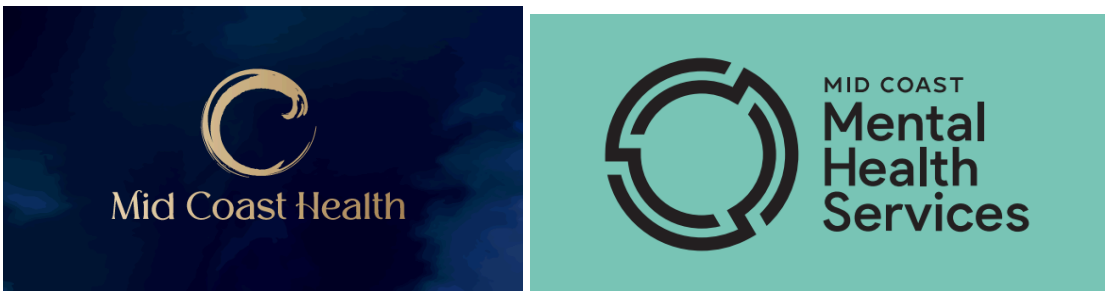
2. Human-Centred Values

- **Policy**: AI systems must respect and promote Australian values of fairness, human rights, and democracy. The business will ensure that AI respects the dignity, autonomy, and rights of all individuals.
- **Implementation**:
    - Integrate human-centred design principles in the development of AI applications.
    - Ensure AI systems do not infringe on individual privacy or autonomy by conducting regular audits and adhering to strict data protection standards.
    - Involve stakeholders, including employees and customers, in the design and deployment of AI to ensure their needs and values are reflected.

3. Fairness

- **Policy**: Businesses must ensure that AI systems are designed and implemented in a fair manner, avoiding bias and discrimination. AI systems should not result in unfair outcomes for individuals or groups.

- **Implementation**:



- Conduct bias assessments on AI algorithms and datasets to detect and mitigate potential biases.
- Establish a diverse team of AI developers and stakeholders to ensure multiple perspectives are considered in AI design.
- Regularly evaluate AI decision-making processes to ensure fairness in outcomes, especially for vulnerable populations.

4. Privacy Protection and Security

- **Policy**: AI systems must protect individuals' privacy and ensure data security. The business will comply with all legal and ethical standards related to data protection.
- **Implementation**:
  - Ensure that all data used in AI applications is collected, stored, and processed in accordance with Australian privacy laws (such as the Privacy Act 1988).
  - Employ robust encryption, access controls, and security protocols to protect sensitive data from unauthorized access or breaches.
  - Develop and enforce a clear data governance framework for AI applications, detailing how data is used, shared, and protected.

5. Reliability and Safety

- **Policy**: AI systems must be reliable and operate safely throughout their lifecycle. Businesses will ensure that AI systems are consistently monitored, tested, and updated to avoid failures or unintended harm.
- **Implementation**:
  - Implement regular testing and validation of AI models to ensure they operate as intended.
  - Establish a monitoring process for detecting anomalies or failures in AI systems and take immediate corrective action.
  - Design AI systems with safety mechanisms, including fallback options that allow human intervention in case of system failure or unpredictability.

6. Transparency and Explainability

- **Policy**: AI systems must be transparent, and their decisions should be explainable. The business will ensure that employees, customers, and stakeholders understand how AI systems work and how decisions are made.
- **Implementation**:
    - Provide clear documentation on how AI systems operate, including the data used, algorithms applied, and decision-making processes.
    - Ensure that AI-generated decisions can be easily explained to non-technical stakeholders, such as employees or customers, in a way that they can understand.
    - Develop tools to track and audit AI decision-making processes for transparency and accountability.

7. Contestability

- **Policy**: Individuals affected by AI decisions must have the ability to challenge and contest those decisions. The business will provide mechanisms for users or stakeholders to appeal AI-driven outcomes.
- **Implementation**:
    - Establish a process for individuals to raise concerns or disputes about AI-driven decisions.
    - Create a review mechanism where AI decisions are regularly audited, and individuals can request manual review or correction of erroneous AI outcomes.
    - Maintain a clear record of AI decision-making processes to facilitate review in contested cases.

8. Accountability

- **Policy**: The business will ensure that AI systems are developed and deployed with clear accountability structures. Employees and departments responsible for AI will be held accountable for the ethical use of these systems.
- **Implementation**:
    - Assign a dedicated AI ethics officer or team to oversee the implementation and ethical compliance of AI systems.
    - Ensure that all AI projects have clear governance structures, including roles and responsibilities for ethical oversight.

- Implement regular audits of AI systems to ensure compliance with ethical standards and address any issues promptly.

Compliance Monitoring and Review

- Conduct regular internal audits to assess adherence to the AI ethics policies.
- Report compliance results to executive leadership on a quarterly basis and provide recommendations for improving the ethical use of AI.
- Engage external consultants to review and provide feedback on the business's AI ethics framework every two years.

This policy ensures businesses are not only complying with the national AI ethics principles but also taking proactive steps to promote fairness, transparency, and accountability in their AI practices.

Client Privacy Policy for Mental Health Nursing Services

Effective Date: 6th September 2024

At Mid Coast Health Pty T/as Mid Coast Mental Health Services (MCMHS), we are committed to ensuring the privacy and confidentiality of our clients' personal and sensitive information, including any recordings or documentation generated during mental health nursing sessions. This policy outlines how we collect, use, store, and protect client data, particularly regarding the use of session recordings, storage of session script documents in Power Diary CRM, and storage on Google Suite platforms.

---

1. Collection of Client Information

We collect personal and health-related information necessary to provide quality mental health nursing services. This information may include:

- Personal details (name, address, contact information).
- Medical history, psychological assessments, and clinical notes.
- Session recordings (if applicable) and session script documents.

All information collected is handled in accordance with the Australian Privacy Principles (APPs) under the **Privacy Act 1988**.

2. Use of Session Recordings

- **Purpose**: Session recordings may be used for clinical review, supervision, training purposes, or for clients' personal records (if applicable).
- **Consent**: Recordings will only be made with the explicit, informed consent of the client. Clients will be informed of the purpose of the recording and how it will be stored and used.
- **Client Rights**: Clients have the right to refuse consent for recordings without any impact on their care or treatment. They can also request that recordings be deleted at any time.

3. Storage of Session Recordings

- **Platform**: If session recordings are made, they will be securely stored using the [insert platform, e.g., Power Diary CRM or Google Drive] and will be encrypted to ensure confidentiality.

- **Security**: Recordings will be protected with multi-factor authentication and encryption to safeguard against unauthorized access. Only authorized personnel will have access to these recordings.
- **Retention Period**: Recordings will be stored for the minimum necessary period, in accordance with applicable laws and clinical guidelines, after which they will be securely deleted.

4. Storage of Session Script Documents

- **Power Diary CRM**: Client session notes and related documents will be stored in Power Diary, a secure practice management platform.
    - **Security Features**: Power Diary uses encryption and meets the highest security standards for healthcare data storage, ensuring that client documents are protected.
    - **Access Controls**: Access to Power Diary is restricted to authorized healthcare professionals within our practice. Each user is required to log in via a secure portal with multi-factor authentication.
    - **Backup and Retention**: Data stored on Power Diary is backed up regularly and retained in accordance with clinical record-keeping guidelines.
- **Google Suite Platforms**: In some cases, session documents may also be stored on Google Drive or within the Google Suite platform.
    - **Security Features**: Google Suite employs strong encryption both in transit and at rest. Only authorized personnel within our practice have access to client data on this platform.
    - **Data Access**: Access is limited to necessary personnel, and all accounts are protected with multi-factor authentication. Data stored in Google Drive is regularly reviewed and managed to ensure privacy compliance.
    - **Sharing and Permissions**: Documents stored in Google Drive will never be shared with unauthorized individuals or third parties without explicit client consent, except where required by law.

5. Use and Disclosure of Information

- **Primary Use**: Client information, including recordings and session scripts, is primarily used to deliver mental health services and ensure continuity of care.

- **Disclosure**: Information will not be shared with third parties without the client's explicit consent, except in situations where disclosure is required by law (e.g., risk of harm to self or others, court orders).

- **External Providers**: In cases where client data needs to be shared with other healthcare providers or external agencies, clients will be informed and their consent obtained, unless an emergency situation exists.

6. Client Rights

- **Access to Information**: Clients have the right to request access to their personal information, including session recordings and documents, at any time. We will provide access in a timely manner, subject to applicable laws and regulations.
- **Correction of Information**: Clients may request corrections to their personal information if they believe it to be inaccurate or incomplete.
- **Withdrawal of Consent**: Clients can withdraw their consent for the storage or use of session recordings and documents at any time. Upon withdrawal, we will take all reasonable steps to delete or return the data, subject to legal and clinical obligations.

7. Data Breach Protocol

- **Security Incidents**: In the unlikely event of a data breach involving client information, including recordings or session documents, we will follow all relevant reporting procedures, including notifying affected clients and regulatory authorities as required by the **Notifiable Data Breaches Scheme**.
- **Response Plan**: Our team is trained to respond promptly to security incidents, and we maintain regular reviews of our systems to prevent breaches.

8. Client Confidentiality

- All employees and contractors involved in providing mental health services are bound by strict confidentiality agreements. Breaches of client confidentiality by any staff member will result in disciplinary action in accordance with our internal policies and the law.

9. Review and Updates to Policy

- This policy will be reviewed regularly to ensure it complies with legal requirements and industry standards for privacy and data protection. Clients will be notified of any significant changes to this policy.

Contact Information

If you have any questions or concerns regarding this privacy policy or how your information is handled, please contact Mick Easton – Director: Mid Coast Health Pty T/as Mid Coast Mental Health Services at:

- **Email**: info@midcoastmhs.com
- **Phone**: 0431193720

By engaging with our services, you agree to this privacy policy, ensuring the protection and confidentiality of your personal information throughout your care with us.

What are privacy safeguards in Power Diary?

Power Diary has implemented several privacy and security safeguards to protect client information and ensure compliance with data protection regulations. These safeguards are designed to maintain the confidentiality, integrity, and availability of sensitive health information. Below are the key privacy safeguards in Power Diary:

1. Data Encryption

- **In-Transit Encryption**: Power Diary encrypts all data transmitted between users and the platform using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols. This ensures that data transferred over the internet cannot be intercepted by unauthorized parties.
- **At-Rest Encryption**: Data stored in Power Diary is encrypted at rest, meaning that even if someone gains access to the storage system, the data will be unreadable without the encryption keys.

2. Role-Based Access Control (RBAC)

- **User Permissions**: Power Diary allows businesses to assign specific roles to users within the system, ensuring that only authorized personnel can access certain types of data. Access is granted based on the user's role (e.g., practitioner, admin), minimizing the risk of unauthorized access to sensitive information.
- **Customizable Permissions**: Administrators can further customize permissions for different users, ensuring that each staff member has access only to the information necessary for their role.

3. Two-Factor Authentication (2FA)

- Power Diary supports two-factor authentication (2FA), which adds an additional layer of security. When 2FA is enabled, users must enter a second form of authentication, such as a code sent to their mobile device, in addition to their password.

4. Data Backups and Redundancy

- **Automated Backups**: Power Diary performs regular automated backups of all client data. This ensures that in the event of a system failure or data breach, no data is lost.

- **Redundant Systems**: The platform uses redundant servers and data centers to ensure high availability and prevent data loss in case of hardware failures or other technical issues.

5. Data Hosting in Secure Locations

- **Secure Data Centers**: Power Diary stores data in highly secure data centers that comply with strict industry standards for data protection. These centers are equipped with physical security measures such as biometric access controls, surveillance systems, and 24/7 monitoring.
- **Compliance with Local Regulations**: Power Diary stores data in compliance with local data protection laws, such as the **Australian Privacy Principles (APPs)** for Australian users, and ensures that data is stored in regions that meet these legal requirements.

6. Audit Logs and Tracking

- **Activity Tracking**: Power Diary maintains detailed logs of user activity within the system, allowing administrators to track who accessed or modified client records. This promotes accountability and transparency, making it easier to detect and investigate any unauthorized access or suspicious activity.
- **Audit Trails**: The platform provides comprehensive audit trails, which can be reviewed to ensure compliance with internal policies and regulatory requirements.

7. Regular Security Audits and Updates

- **Security Audits**: Power Diary undergoes regular security audits to identify vulnerabilities and ensure that the system is adhering to the highest security standards.
- **Software Updates**: The platform is regularly updated with the latest security patches and improvements to protect against new and emerging threats.

8. Data Ownership and Control

- **Client Data Ownership**: Power Diary ensures that its users (the healthcare providers) maintain full ownership of all client data. This means that users can access, export, and delete their data at any time, complying with data protection regulations such as GDPR (for European users).
- **Client Data Portability**: Power Diary supports data portability, enabling healthcare providers to export client records if they need to switch to another system or maintain backup copies for regulatory compliance.

9. Compliance with Privacy Regulations

- Power Diary is designed to comply with various privacy and data protection laws, including:
    - **Australian Privacy Principles (APPs)** for businesses in Australia.
    - **General Data Protection Regulation (GDPR)** for businesses serving European clients.
    - **Health Insurance Portability and Accountability Act (HIPAA)** for businesses in the United States that handle protected health information (PHI).

10. Client Confidentiality and Consent Management

- **Consent Management**: Power Diary allows users to document and manage client consent for the collection and use of personal health information. This ensures that clients are informed about how their data is used and have provided explicit consent where required.
- **Confidentiality Controls**: The platform supports various confidentiality controls to ensure that sensitive client information is only accessible by authorized individuals within the practice.

These safeguards ensure that Power Diary maintains a high level of security, protecting client data from unauthorized access and ensuring compliance with applicable privacy laws and regulations.

What are Google Suite's privacy safeguards?

Google Workspace

Google Suite (now known as Google Workspace) offers a range of privacy safeguards designed to protect the data and privacy of its users, including businesses and organizations that handle sensitive information. Here are the key privacy safeguards implemented by Google Suite:

1. Data Encryption

- **In-Transit Encryption**: Google Workspace encrypts all data during transit between your device and Google's servers using Transport Layer Security (TLS). This ensures that data cannot be intercepted or altered during transmission.
- **At-Rest Encryption**: Data stored on Google's servers is encrypted at rest using strong encryption standards such as 256-bit Advanced Encryption Standard (AES). This ensures that data remains protected from unauthorized access even when stored.

2. Two-Factor Authentication (2FA)

- **Enhanced Security with 2FA**: Google Workspace supports two-factor authentication (2FA), adding an extra layer of protection to user accounts. Users must verify their identity with a second factor, such as a text message code or an authenticator app, in addition to their password.
- **Security Key Support**: Google also supports hardware security keys as part of its two-factor authentication process, providing an additional layer of defense against phishing and account breaches.

3. Data Access and Control

- **Role-Based Access Controls (RBAC)**: Administrators can control who has access to specific data by assigning roles and setting permissions within Google Workspace. This minimizes the risk of unauthorized access by limiting access to those who need it.
- **Granular Sharing Permissions**: Google Workspace offers detailed sharing settings, allowing users to control who can view, comment, or edit documents. Admins can also prevent external sharing of sensitive documents and enforce company-wide sharing policies.

4. Privacy and Confidentiality by Design

- **Data Ownership**: Google Workspace ensures that businesses retain full ownership of their data. Google does not use customer data for advertising purposes and provides full transparency about how data is processed and stored.
- **Client-Side Encryption**: Google offers client-side encryption, which allows businesses to control encryption keys and ensure that even Google cannot access the encrypted content of documents stored in Google Drive.

5. Compliance with Data Protection Regulations

- **GDPR Compliance**: Google Workspace complies with the General Data Protection Regulation (GDPR), ensuring that businesses operating in the European Union can manage and protect personal data in accordance with the law.
- **HIPAA Compliance**: For healthcare organizations, Google Workspace can be configured to comply with the Health Insurance Portability and Accountability Act (HIPAA), which governs the protection of sensitive health information.
- **SOC 2, SOC 3, and ISO Certifications**: Google Workspace meets key security and privacy standards, including SOC 2, SOC 3, and ISO/IEC 27001 certifications, which demonstrate its commitment to protecting data.

6. Data Loss Prevention (DLP)

- **DLP Policies**: Google Workspace offers built-in data loss prevention (DLP) tools to prevent sensitive information from being shared or accessed inappropriately. Administrators can set rules to detect and block sensitive data, such as credit card numbers or personal health information, before it is sent via email or shared externally.
- **Email DLP**: Gmail within Google Workspace has DLP rules that can scan outgoing emails and attachments for sensitive information, allowing administrators to block or quarantine messages that violate security policies.

7. Data Retention and Archiving

- **Google Vault**: Google Workspace offers Google Vault for data retention, e-discovery, and archiving. Administrators can set retention policies for emails, chat messages, and files to ensure compliance with legal and regulatory requirements.
- **Backup and Recovery**: Google Workspace data is regularly backed up, and users can recover deleted emails or files within a specified retention period. This ensures data availability even in case of accidental deletions.

8. Regular Security Audits and Updates

- **Security Audits**: Google conducts regular internal and external security audits to ensure that its infrastructure and services meet the highest security standards. Google continuously monitors and evaluates its security controls.
- **Automatic Updates**: Google Workspace automatically receives security patches and updates, ensuring that systems remain up to date with the latest security features and threat defenses.

9. Transparency and Control Over Data Usage

- **Activity Logs and Audit Reports**: Google Workspace provides administrators with detailed logs and audit reports to track user activities, such as document access, sharing, and sign-ins. These logs allow businesses to monitor potential security incidents and investigate any suspicious activity.
- **Admin Console**: The Google Admin Console offers full control over how data is managed and stored. Administrators can configure security settings, manage devices, and review audit reports from a single interface.

10. Security Center and Alerts

- **Google Workspace Security Center**: This feature provides businesses with a unified view of their security status, allowing them to monitor threats and vulnerabilities across their organization. The security center also provides actionable insights and best practices to improve data protection.
- **Security Alerts**: Google Workspace notifies administrators of any potential security issues, such as suspicious sign-ins or compromised accounts. Administrators can set up custom alerts and monitor real-time security incidents.

11. Data Portability

- **Portability and Export Tools**: Google Workspace allows businesses to export their data at any time using Google Takeout or the Admin Console. This ensures that businesses have control over their data and can move it to another platform if needed.

12. Incident Response and Data Breach Notifications

- **Incident Response Team**: Google has a dedicated incident response team that monitors systems 24/7 for security threats and takes immediate action in the event of a data breach.
- **Breach Notification**: In compliance with data protection regulations, Google notifies affected customers and authorities in the event of a data breach involving personal information.

Summary:

Google Suite (Google Workspace) ensures privacy through strong encryption (in-transit and at-rest), two-factor authentication, granular access controls, and compliance with major data protection regulations like GDPR and HIPAA. It offers tools for data loss prevention, data retention, and auditing, ensuring that businesses have complete control and visibility over their data. Additionally, Google's regular security audits, transparency in data usage, and incident response mechanisms further bolster the protection of client data.

Privacy Summary Statement for Mid Coast Health Pty (MCMHS)

At Mid Coast Health Pty, trading as Mid Coast Mental Health Services (MCMHS), we are committed to ensuring the privacy, security, and accuracy of all client data in accordance with industry best practices and applicable regulations. Our use of Google Workspace and Power Diary platforms, as well as our adherence to ethical AI principles, reflects our dedication to safeguarding client information through robust encryption, access control, and transparency.

- **Google Workspace**: MCMHS uses Google Workspace for the secure storage and management of documents. Google Workspace ensures that all data is encrypted both in transit and at rest, and that access to information is restricted to authorized personnel only. We employ two-factor authentication (2FA) and data loss prevention (DLP) tools to prevent unauthorized access and sharing of sensitive client information. Regular security updates and compliance with GDPR and HIPAA regulations reinforce the privacy and security of the data we handle.
- **Power Diary**: Our practice management system, Power Diary, is designed to meet stringent healthcare data protection requirements. All client data, including session notes and health records, are securely stored with encryption and protected by role-based access controls. Power Diary's audit logs allow us to monitor and track access to client records, ensuring full accountability and transparency in how we manage client data.
- **AI Use and Ethical Compliance**: MCMHS is committed to using AI technologies in a manner that aligns with Australia's AI Ethics Principles. We ensure that AI systems prioritize human-centred values, fairness, privacy protection, and transparency. Any AI systems we deploy are continuously monitored for reliability and safety, and we provide clients with the ability to contest decisions made by AI-driven processes.

At MCMHS, we operate in an open and transparent manner, ensuring that all clients are informed of how their data is collected, stored, and used. We regularly review and update our privacy practices to maintain the accuracy and integrity of client information, and we take immediate action to correct any errors. Our commitment to privacy extends to providing clients with full control over their personal data, allowing them to access, correct, or request the deletion of their information at any time.

Through these safeguards, MCMHS ensures that client data is handled with the utmost care and confidentiality, in compliance with Australian privacy laws and ethical standards.