Privacy and Confidentiality Policy

Version: 1.0

Commencement Date: 12 January 2025

Review Date: 12 January 2025

Please note that printed and saved copies of this document are considered uncontrolled. For the most up-to-date version, please visit www.workinganimals.com.au

Citation:
Working Animals Federation of Australia (WAFA), “Privacy and Confidentiality Policy”, Version 1.0, January 12 2025, www.workinganimals.com.au/policies

Contents

1. Purpose

Our privacy and confidentiality policy is designed to safeguard the personal and sensitive information entrusted to us by our clients, employees, partners, and other stakeholders. We are committed to maintaining the highest standards of privacy protection and confidentiality across all aspects of our operations. This policy serves as a framework to guide our practices in collecting, storing, processing, and sharing data, ensuring compliance with relevant laws and regulations while fostering trust and transparency with those who rely on us.

2. Scope

This privacy and confidentiality policy applies to all individuals and entities associated with our organisation, including but not limited to:

1. Staff: This encompasses all employees, contractors, consultants, and temporary workers engaged by our organisation, regardless of their role or position.

2. Volunteers: Volunteers contributing their time and effort to our organisation are also covered by this policy, ensuring that their personal information and contributions are treated with utmost respect and confidentiality.

3. Steering Committee: Members of the steering committee, responsible for guiding strategic decisions and governance, are included within the scope of this policy to ensure that their personal and sensitive information is protected.

4. Clients: Whether current, former, or prospective clients, this policy extends to all individuals and organisations that engage with our services, ensuring the confidentiality of their personal and business-related information.

5. Supporting and Financial Members: Individuals or entities providing financial support or membership to our organisation fall within the scope of this policy, safeguarding their personal details and financial transactions.

6. Certified Members: Any individuals certified by our organisation or affiliated certification bodies are covered by this policy, protecting their personal and professional information related to certification processes.

7. Other Stakeholders: This policy also extends to any other individuals or entities interacting with our organisation, such as partners, suppliers, sponsors, and collaborators, ensuring their privacy and confidentiality are respected.

8. Collaborators: This policy extends to anyone supplying information in a collaborative nature (for example on online platforms).

In summary, this policy applies comprehensively to all individuals and entities involved in any capacity with our organisation, emphasising our commitment to upholding privacy and confidentiality standards across the board.

3. Policy Statement:

Working Animals Federation of Australia (WAFA) is committed to upholding the highest standards of privacy protection and confidentiality across all facets of our operations. We recognise the importance of safeguarding personal and sensitive information entrusted to us by all stakeholders. This policy is in alignment with the *Privacy Act 1988 (Cth),* which includes the Australian Privacy Principles (APPs).

We affirm our dedication to:

1. Respecting Privacy Rights: We respect the privacy rights of individuals associated with our organisation and are committed to protecting their personal information from unauthorised access, use, or disclosure.

2. Maintaining Confidentiality: We acknowledge the confidential nature of the information entrusted to us and are dedicated to maintaining its confidentiality, ensuring that it is accessed and used only for legitimate purposes.

3. Compliance: We adhere to all applicable privacy laws and regulations, as well as industry standards and best practices, to ensure compliance with legal requirements and promote transparency in our data handling practices.

4. Accountability: We hold ourselves accountable for the protection of personal and sensitive information within our possession or control, implementing appropriate safeguards to mitigate risks and prevent unauthorized access or disclosure.

5. Transparency: We strive to be transparent about our data handling practices, providing clear information to individuals about how their information is collected, used, and protected.

6. Continuous Improvement: We are committed to continuously improving our privacy and confidentiality practices through regular review, assessment, and enhancement of our policies, procedures, and security measures.

By adhering to this policy and related internal procedures and processes, we aim to foster trust, confidence, and respect among all stakeholders, and demonstrate our unwavering commitment to upholding their privacy and confidentiality rights.

4. Definitions

Key Terms and Concepts:

1. Personal Information: Any information that relates to an identified or identifiable individual. This may include but is not limited to, names, contact details, identification numbers, financial information, health information, and any other information that can be linked to a specific person.

2. Sensitive Information: Information that requires a higher level of protection due to its potential to cause harm or embarrassment if disclosed without authorisation. This may include, but is not limited to, information related to an individual's race, ethnicity, religion, political beliefs, health status, sexual orientation, criminal history, or financial information.

3. Confidential Information: Information that is treated with a higher level of confidentiality due to its sensitive or proprietary nature. This may include, but is not limited to, trade secrets, intellectual property, strategic plans, financial data, customer lists, and any other information that is not intended for public disclosure.

4. Data Handling: The process of collecting, storing, processing, transmitting, and disposing of data in accordance with established policies, procedures, and security measures.

5. Compliance: Adherence to relevant laws, regulations, standards, and internal processes governing the collection, use, and protection of personal and sensitive information.

6. Accountability: The principle of being answerable for one's actions and decisions related to the handling of personal and sensitive information, including taking responsibility for any breaches or violations of privacy and confidentiality policies.

7. Transparency: Openness and honesty in communicating with individuals about the collection, use, and protection of their personal and sensitive information, including providing clear and understandable information about data handling practices.

8. Continuous Improvement: The ongoing process of evaluating, refining, and enhancing privacy and confidentiality practices to adapt to evolving threats, technologies, and regulatory requirements, thereby ensuring the highest level of protection for personal and sensitive information.

5. Responsibilities

Each party is responsible for implementing and adhering to the privacy and confidentiality policy to promote a culture of accountability, transparency, and trust in its data handling practices.

Responsibilities of Various Parties in Implementing and Adhering to the Policy:

1. Steering Committee:

- Establish and maintain the overarching privacy and confidentiality policy framework.
- Provide oversight and direction for the implementation of privacy and confidentiality practices.
- Allocate resources and support necessary for compliance with the policy.
- Review and approve any updates or revisions to the policy as needed.
- Ensure that privacy and confidentiality considerations are integrated into organisational decision-making processes.

2. Staff:

- Familiarize themselves with the organisation's privacy and confidentiality policy and procedures.
- Handle personal and sensitive information in accordance with established policies and procedures.
- Participate in privacy and confidentiality training and awareness programs provided by the organisation.
- Report any suspected breaches or violations of the policy to designated authorities.
- Cooperate with investigations and audits related to privacy and confidentiality compliance.

3. Volunteers:

- Adhere to the organisation's privacy and confidentiality policy and procedures.
- Handle personal and sensitive information with the same level of care as staff members.
- Seek guidance and clarification from staff or designated authorities if unsure about privacy and confidentiality requirements.
- Report any breaches or violations of the policy observed during their volunteer activities.

4. Compliance Officer:

- Serve as the primary point of contact for privacy and confidentiality-related inquiries and concerns.
- Develop and implement privacy and confidentiality training programs for staff and volunteers.
- Monitor compliance with the policy and investigate any suspected breaches or violations.

- Maintain records of privacy and confidentiality incidents, investigations, and corrective actions taken.
- Provide regular reports to the steering committee or senior management on privacy and confidentiality compliance efforts.

5. Human Resources Department:

- Ensure that privacy and confidentiality policies and procedures are included in employee onboarding and training programs.
- Manage access controls and permissions for personal and sensitive information in accordance with organisational policies.
- Handle privacy-related inquiries and requests from employees and other stakeholders.
- Coordinate with the compliance officer or privacy officer to address privacy and confidentiality issues as they arise.

6. Information Technology (IT) Department:

- Implement technical safeguards and security measures to protect personal and sensitive information from unauthorized access, use, or disclosure.
- Monitor and audit system access logs and activity to detect and prevent security breaches.
- Provide technical support and guidance to staff and volunteers on secure data handling practices.
- Ensure that data backups and disaster recovery plans are in place to minimize the impact of data breaches or loss.

6. Procedures

By following these steps and implementing the necessary processes, forms, and documentation, the organisation can effectively comply with its privacy and confidentiality policy, safeguarding the personal and sensitive information entrusted to its care.

Steps to Comply with the Privacy and Confidentiality Policy:

1. Awareness and Training:

- All staff, volunteers, and relevant stakeholders are required to undergo comprehensive training on the organisation's privacy and confidentiality policy and procedures.
- Training sessions should cover topics such as data handling best practices, security protocols, and privacy rights.
- Records of training attendance and completion should be maintained by the Human Resources Department or designated compliance officer.

2. Data Collection and Consent:

- Clearly define the purposes for which personal and sensitive information will be collected and obtain consent from individuals before collecting their data.
- Develop standardized consent forms or processes for individuals to provide explicit consent for the collection, use, and disclosure of their information.
- Ensure that individuals are informed about their privacy rights, including the right to access, correct, or delete their personal information.

3. Data Storage and Security:

- Establish secure storage mechanisms for personal and sensitive information, such as encrypted databases or password-protected systems.
- Implement access controls and permissions to limit access to personal and sensitive information only to authorized personnel who require it for their job duties.
- Regularly review and update security measures to address emerging threats and vulnerabilities.
- Maintain an inventory of all personal and sensitive information held by the organisation, including its location, purpose, and access controls.

4. Data Use and Disclosure:

- Limit the use and disclosure of personal and sensitive information to purposes that are consistent with the consent provided by individuals or as required by law.
- Develop procedures for securely sharing information with third parties, such as partners, vendors, or service providers, while ensuring that appropriate confidentiality agreements are in place.
- Obtain explicit consent from individuals before disclosing their information to third parties for purposes not covered by the original consent.

5. Data Retention and Disposal:

- Establish retention periods for different types of personal and sensitive information based on legal requirements, organisational needs, and the purposes for which the data was collected.
- Develop procedures for securely disposing of personal and sensitive information once it is no longer needed, including shredding paper documents and securely deleting electronic files.
- Maintain records of data retention and disposal activities to demonstrate compliance with privacy and confidentiality requirements.

6. Incident Response and Reporting:

- Develop a formal incident response plan to address data breaches, unauthorized disclosures, or other privacy and confidentiality incidents.
- Designate a response team responsible for investigating incidents, mitigating risks, and implementing corrective actions.
- Establish procedures for reporting privacy and confidentiality incidents to regulatory authorities, affected individuals, and other relevant stakeholders as required by law.

7. Monitoring and Review:

- Conduct regular audits and assessments of privacy and confidentiality practices to identify areas for improvement and ensure ongoing compliance with the policy.
- Review and update the privacy and confidentiality policy and procedures as needed to reflect changes in laws, regulations, or organisational practices.
- Maintain documentation of compliance efforts, including audit reports, policy updates, and training records, to demonstrate adherence to privacy and confidentiality requirements.

7. Compliance

By aligning with relevant federal and NSW privacy laws, regulations, and standards, the organisation's privacy and confidentiality policy ensures compliance with legal requirements for the protection of personal information. Compliance will be monitored and enforced through a combination of internal audits, assessments, training programs, and incident response protocols to uphold the privacy rights of individuals and maintain trust in the organisation's data handling practices.

Legal Requirements and Compliance Monitoring:

1. *Privacy Act 1988 (Cth)* (Australia):
   - The organisation's privacy and confidentiality policy aligns with the Privacy Act 1988 (Cth), which regulates the handling of personal information by Australian government agencies and businesses.

- Compliance with the Privacy Act will be monitored and enforced through regular audits and assessments of privacy and confidentiality practices to ensure adherence to the principles outlined in the legislation.
- The organisation will appoint a compliance officer responsible for overseeing privacy compliance efforts and addressing any breaches or violations of the Privacy Act.

2. Australian Privacy Principles (APPs):
- The organisation's privacy and confidentiality policy complies with the Australian Privacy Principles (APPs), which set out the standards, rights, and obligations for handling personal information under the Privacy Act.
- Compliance with the APPs will be monitored through internal audits, assessments, and reviews of data handling practices to ensure alignment with the principles outlined in the legislation.
- Staff and volunteers will receive training on the APPs to ensure understanding and compliance with the requirements for handling personal information.

3. *Health Records and Information Privacy Act 2002 (NSW)* (HRIPA):
- For organisations handling health-related information in New South Wales (NSW), compliance with the Health Records and Information Privacy Act 2002 (HRIPA) will also be necessary.
- The organisation's privacy and confidentiality policy will include specific provisions to ensure compliance with HRIPA requirements for the handling of health information, such as obtaining consent for collection, use, and disclosure of health records.
- Monitoring and enforcement of HRIPA compliance will be integrated into overall privacy compliance efforts, with regular assessments and audits conducted to ensure adherence to the legislation's requirements.

4. Notifiable Data Breaches Scheme (Australia):
- The organisation will comply with the Notifiable Data Breaches (NDB) scheme under the *Privacy Act*, which requires organisations to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of eligible data breaches.
- Procedures for responding to data breaches, including notification requirements and incident response protocols, will be outlined in the organisation's privacy and confidentiality policy.
- Compliance with the NDB scheme will be monitored through incident response drills, internal reporting mechanisms, and audits to ensure timely and appropriate handling of data breaches in accordance with legal requirements.

8. Training and Communication

interactive workshops, and compliance mechanisms, employees will be well-informed about the privacy and confidentiality policy and equipped to adhere to its requirements in their day-to-day activities. Regular reinforcement and ongoing support will ensure that privacy and confidentiality remain a priority throughout the organisation.

Employees will be informed about the privacy and confidentiality policy through a comprehensive communication and training program designed to ensure understanding and compliance. The following strategies will be employed to effectively disseminate the policy:

1. Training Programs:

- A structured training program will be developed to educate employees about the organisation's privacy and confidentiality policy.
- Training sessions will be conducted by designated trainers, such as the compliance officer or human resources personnel, either in-person or through online modules.
- Training content will cover key aspects of the policy, including data handling best practices, privacy rights, security protocols, and procedures for handling personal and sensitive information.

2. Communication Channels:

- The policy will be distributed to all employees via email, intranet, or other internal communication channels to ensure widespread awareness.
- Regular reminders and updates about the policy will be communicated through team meetings, newsletters, or bulletin boards to reinforce its importance and relevance to employees' roles and responsibilities.

3. Resources Provided:

- A dedicated section on the organisation's intranet or internal portal will be created to serve as a centralized resource hub for the privacy and confidentiality policy.
- Employees will have access to downloadable copies of the policy, training materials, FAQs, and other relevant resources to support their understanding and implementation of the policy.
- Contact information for designated privacy officers or compliance personnel will be provided for employees to seek clarification or assistance regarding the policy.

4. Interactive Workshops and Discussions:

- In addition to formal training sessions, interactive workshops and discussions may be organized to facilitate deeper engagement and understanding of the policy.
- Case studies, scenarios, and real-life examples relevant to employees' roles and responsibilities may be used to illustrate the practical application of the policy in various contexts.

5. Acknowledgement and Compliance:

- Employees will be required to acknowledge receipt and understanding of the policy through a formal acknowledgement form or online attestation process.
- Compliance with the policy will be included as part of employees' performance evaluations and adherence to organisational values and standards.

By employing a combination of training programs, communication channels, resources,

9. Review, Revision and Approvals

Review and Update Process for the Privacy and Confidentiality Policy:

1. Regular Review Schedule:
   - The privacy and confidentiality policy will undergo annual review to ensure its continued effectiveness and relevance.
   - The privacy and confidentiality policy will undergo unscheduled review where changes to legislation or work practices are identified by the compliance officer or HR.

2. Review Committee:
   - A review committee will be appointed by the steering committee to oversee the policy review process.
   - The review committee will comprise individuals with expertise in privacy, legal compliance, risk management, and relevant organisational stakeholders.

3. Data Gathering and Analysis:
   - The review committee will gather feedback and input from key stakeholders, including employees, volunteers, clients, and regulatory authorities, to assess the policy's performance and identify areas for improvement.
   - Data analysis will be conducted to evaluate the effectiveness of current policy provisions, identify emerging privacy risks or trends, and benchmark against industry standards and best practices.

4. Revision and Drafting:
   - Based on the findings of the review process, the review committee will propose revisions and updates to the policy as necessary.
   - Draft revisions will be developed, incorporating feedback and recommendations from stakeholders and aligning with relevant legal requirements and organisational objectives.

5. Consultation and Feedback:
   - Draft revisions will be circulated for internal consultation and feedback among employees, volunteers, and other relevant stakeholders.
   - Feedback will be collected and considered by the review committee to ensure that diverse perspectives are taken into account in the policy revision process.

6. Approval Process:
   - The revised policy will be submitted to the steering committee for approval.
   - The steering committee will review the proposed revisions, consider any feedback or recommendations from the review committee, and make a determination on whether to approve the updated policy.

7. Signatures and Documentation:
   - Once approved by the steering committee, the updated policy will be signed by the appropriate senior executive or designated authority.
   - Signed copies of the policy will be distributed to all employees and stakeholders, and the revised policy will be officially implemented within the organisation.

By following this structured review and update process, the organisation can ensure that its privacy and confidentiality policy remains current, effective, and aligned with evolving legal requirements and organisational needs. The involvement of key stakeholders and the oversight of the steering committee will contribute to the robustness and credibility of the policy revision process.

10. References

Relevant Documents, Legislation, and Resources Supporting the Privacy and Confidentiality Policy:

1. Privacy Act 1988 (Cth) - The primary legislation governing the handling of personal information by Australian government agencies and businesses, providing the framework for privacy protection in Australia.

2. Australian Privacy Principles (APPs) - The set of principles outlined in Schedule 1 of the Privacy Act, which regulate the collection, use, and disclosure of personal information by organisations covered by the Act.

3. Health Records and Information Privacy Act 2002 (NSW) (HRIPA) - Legislation specific to New South Wales (NSW) that regulates the handling of health information by public and private sector organisations, including requirements for consent, access, and security of health records.

4. Notifiable Data Breaches Scheme - Legislation under the Privacy Act that requires organisations to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of eligible data breaches, enhancing transparency and accountability in data handling practices.

5. OAIC Guidance and Resources - The Office of the Australian Information Commissioner provides a range of guidance materials, resources, and best practice recommendations to assist organisations in understanding and complying with privacy laws and regulations.

6. Industry Standards and Best Practices - Relevant industry standards, codes of practice, and guidelines published by industry associations, professional bodies, or regulatory authorities may provide additional guidance and insights into privacy and confidentiality best practices specific to the organisation's sector or industry.

7. Internal Policies and Procedures - Any internal policies, procedures, or guidelines developed by the organisation to supplement the privacy and confidentiality policy and provide specific guidance on data handling practices, incident response protocols, and compliance requirements.

By leveraging these documents, legislation, and resources, the organisation can enhance the effectiveness of its privacy and confidentiality policy and ensure alignment with legal requirements, industry standards, and best practices in data protection and privacy management.

12. Implementation

Steps to Implement the Privacy and Confidentiality Policy:

1. Policy Development:
   - Develop a comprehensive privacy and confidentiality policy that outlines the organisation's commitment to protecting personal and sensitive information and establishes clear guidelines for data handling practices.

2. Dissemination to Relevant Parties:
   - Distribute the policy to all relevant parties, including staff, volunteers, steering committee members, clients, supporting and financial members, certified members, and other stakeholders.
   - Ensure that the policy is accessible through multiple channels, such as the organisation's intranet, email, employee handbooks, and other communication platforms.

3. Training and Awareness Programs:
   - Conduct training sessions to educate employees, volunteers, and other relevant parties about the policy's requirements, expectations, and implications for their roles and responsibilities.
   - Provide training materials, such as presentations, videos, or interactive modules, to facilitate understanding and engagement with the policy.
   - Offer opportunities for questions, discussions, and clarification during training sessions to address any concerns or uncertainties.

4. Support and Guidance:
   - Establish channels for employees and stakeholders to seek support and guidance on privacy and confidentiality matters, such as designated privacy officers, compliance personnel, or helplines.
   - Provide resources, such as FAQs, guidance documents, and contact information for privacy officers, to assist individuals in understanding and implementing the policy in their day-to-day activities.

5. Integration into Organisational Processes:

- Integrate the privacy and confidentiality policy into existing organisational processes, procedures, and workflows to ensure consistent adherence and enforcement.
- Update relevant documents, forms, and agreements to reflect the policy's requirements and incorporate privacy considerations into decision-making processes.

6. Monitoring and Enforcement:
- Establish mechanisms for monitoring compliance with the policy, such as regular audits, assessments, and reviews of data handling practices.
- Implement consequences for non-compliance with the policy, such as disciplinary actions or corrective measures, to reinforce the importance of privacy and confidentiality obligations.

7. Continuous Improvement:
- Foster a culture of continuous improvement by soliciting feedback from employees, volunteers, and stakeholders on the effectiveness of the policy and opportunities for enhancement.
- Regularly review and update the policy in response to changes in laws, regulations, technology, and organisational needs to ensure its continued relevance and effectiveness.

By following these steps, the organisation can effectively implement the privacy and confidentiality policy, foster a culture of privacy awareness and compliance, and safeguard the personal and sensitive information entrusted to its care.

13. Enforcement

The WAFA takes a bast practice approach to privacy and confidentiality, with a focus on prevention through the proactive provision of education and training.

Consequences of Non-Compliance with the Privacy and Confidentiality Policy:

1. Disciplinary and Corrective Actions:
- Employees, volunteers, or other relevant parties found to be in violation of the privacy and confidentiality policy may face disciplinary actions as per the organisation's disciplinary procedures.
- Individuals found to be in non-compliance with the policy may be required to undertake corrective measures to rectify the situation and prevent future violations. Corrective measures may include additional training, counselling, or coaching to improve understanding and adherence to the policy's requirements.
- Individuals may also be required to participate in remedial actions, such as implementing additional safeguards or controls to mitigate risks and prevent recurrence of the non-compliance.
- Disciplinary actions may range from verbal warnings and written reprimands to suspension, demotion, or termination of employment or affiliation with the organisation, depending on the severity of the violation and the individual's history of compliance.

2 Legal and Regulatory Consequences:
- Non-compliance with the privacy and confidentiality policy may result in legal and regulatory consequences, including fines, penalties, or legal proceedings initiated by regulatory authorities or affected individuals.
- Organisations found to be in breach of privacy laws or regulations may face sanctions, enforcement actions, or reputational damage, impacting their credibility, trustworthiness, and viability in the marketplace.

3. Reputational Damage:
- Non-compliance with the privacy and confidentiality policy can damage the organisation's reputation and erode trust among stakeholders, including employees, clients, partners, and the broader community.
- Negative publicity, media coverage, or public scrutiny resulting from privacy breaches or violations can tarnish the organisation's brand image and undermine its standing in the marketplace.

4. Financial Losses:
- Privacy breaches or violations can result in financial losses for the organisation, including costs associated with remediation efforts, legal fees, regulatory fines, settlements, and damage to business relationships.
- Loss of customers, clients, or donors due to concerns about privacy and data security can also impact the organisation's revenue and financial sustainability.

Overall, non-compliance with the privacy and confidentiality policy can have serious consequences for individuals, organisations, and stakeholders involved. Therefore, it is essential for all parties to understand and adhere to the policy's requirements to mitigate risks, maintain trust, and uphold the organisation's commitment to protecting personal and sensitive information.

14. Contact Information

Contact Information for Further Assistance:

For further information or assistance related to the privacy and confidentiality policy, please contact the steering committee at the following email address:

Email: admin@workinganimals.com.au

The steering committee will be able to provide additional guidance, clarification, or support regarding the organisation's privacy and confidentiality policy, as well as address any inquiries or concerns related to data handling practices. Please feel free to reach out to them with any questions or feedback you may have.