



## Professional Standard 4 - Data Storage and Privacy (Summary)

Version: 1.0

Commencement Date: 17 May 2025

Review Date: 17 May 2026

-----  
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](http://www.workinganimals.com.au)

Full versions of WAFA Professional Standards are controlled documents and available only to those enrolled in or graduated from a WAFA credential. Access may also be granted to government agencies and approved research groups upon request. For enquiries, please contact [admin@workinganimals.com.au](mailto:admin@workinganimals.com.au)

-----

### Citation:

Working Animals Federation of Australia (WAFA), "Professional Standard 4 - Data Storage and Privacy (Summary)," Version 1.0 May 17, 2025, [www.workinganimals.com.au/standards](http://www.workinganimals.com.au/standards)

## Professional Standard 8 - Data Storage and Privacy (Summary)

### 1. Purpose

The purpose of this standard is to ensure that all WAFA members handle personal and sensitive information ethically, securely, and in full compliance with Australian privacy law. This includes safeguarding the dignity, safety, and autonomy of individuals—particularly people with disability and those in vulnerable circumstances—through responsible information management. The standard aims to build trust, uphold human rights, and provide clear expectations for data collection, consent, use, sharing, and storage. It reinforces WAFA's commitment to transparency, accountability, and lawful practice in all aspects of service delivery and organisational conduct.

### 2. Scope

These standards apply to all WAFA-accredited individuals and organisations responsible for the training, placement, husbandry, assessment, retirement, or oversight of working animals. This includes professional trainers, volunteers, foster carers, breeders, and handlers. They apply across all working animal species recognised under WAFA.

### 3. Standard Statement

WAFA members must uphold exemplary standards of animal care, training, and wellbeing. Training must be delivered by qualified personnel using humane, evidence-based methods. Animals must be raised, socialised, trained and worked in environments that promote resilience, confidence, and public safety. Members must ensure animals perform specific tasks and pass robust readiness and reassessment procedures. Ongoing welfare, handler training, and retirement planning are required to ensure ethical and sustainable practices.

### 4. Definitions

- **Personal Information:** Information or opinion (true or not) about an identified individual, or an individual who is reasonably identifiable. Examples include names, addresses, contact details, and photographs.
- **Sensitive Information:** A subtype of personal information including racial or ethnic origin, political opinions, religion, trade union membership, sexual orientation, criminal records, or health/disability data.
- **Health Information:** A type of sensitive information that includes any data about a person's health, disability, use of health services, or medical history.
- **Data Breach:** An incident in which personal or sensitive information is lost, accessed, disclosed, or altered without authorisation, whether accidental or malicious.
- **Consent:** Voluntary, informed, specific, and current agreement to the handling of personal information. Consent may be written, verbal, or implied, but must be documented wherever possible.
- **Australian Privacy Principles (APPs):** The 13 legally binding principles under the *Privacy Act 1988 (Cth)* that regulate the handling of personal information by organisations covered by the Act.

- **APP Entity:** An agency or organisation (including WAFA members) that is bound by the *Privacy Act 1988* and must comply with the APPs.
- **Anonymisation:** The process of permanently removing all personally identifiable elements from a dataset so individuals cannot be identified.
- **De-identification (Pseudonymisation):** The removal or alteration of personal identifiers to reduce the risk of identification, while potentially allowing re-identification if necessary for legitimate reasons.
- **Privacy Impact Assessment (PIA):** A formal risk management process used to identify and minimise the privacy impacts of new projects, technologies, or data-handling activities.

## 5. Roles and Responsibilities

- **Board:** Responsible for governance, setting strategic direction, risk management, financial oversight, and compliance with WAFA standards.
- **Senior Leadership:** Implements board policies and manages day-to-day operations.
- **Staff and Volunteers:** Support organisational objectives under leadership direction and adhere to governance policies.

### 8.1 Commitment to Privacy

WAFA members must uphold the highest standards of data privacy, confidentiality, and ethical data stewardship when collecting, storing, using, or disclosing any personal, sensitive, or health-related information concerning handlers, animals, clients, staff, volunteers, or stakeholders.

Privacy is both a legal obligation and an ethical responsibility, especially in contexts involving disability, health vulnerability, or marginalised communities.

### 8.2 Compliance with Australian Privacy Law

WAFA members must comply with the *Privacy Act 1988 (Cth)*, including the 13 Australian Privacy Principles (APPs). These apply to any organisation:

- With annual turnover > \$3 million
- Providing health services
- Handling health information
- Receiving Commonwealth funding (e.g. via NDIS)

Regardless of legal threshold, all WAFA members are expected to apply the APPs as best practice.

## The 13 Australian Privacy Principles (APPs):

### 1. APP 1 – Open and Transparent Management of Personal Information

Maintain a clear privacy policy and manage personal information transparently.

2. **APP 2 – Anonymity and Pseudonymity**  
Allow individuals to remain anonymous or use a pseudonym where lawful and practicable.
3. **APP 3 – Collection of Solicited Personal Information**  
Collect only necessary information by lawful and fair means.
4. **APP 4 – Dealing with Unsolicited Personal Information**  
Destroy or de-identify unsolicited data unless legally required to keep it.
5. **APP 5 – Notification of Collection**  
Inform individuals why and how their data is being collected at the time of collection.
6. **APP 6 – Use or Disclosure of Personal Information**  
Only use or share data for the original purpose or a directly related purpose the person would expect.
7. **APP 7 – Direct Marketing**  
Use personal information for marketing only with proper consent and opt-out mechanisms.
8. **APP 8 – Cross-border Disclosure of Personal Information**  
Ensure overseas recipients uphold privacy standards equivalent to Australia's.
9. **APP 9 – Adoption, Use or Disclosure of Government Identifiers**  
Do not use government-issued identifiers (e.g., Medicare numbers) as internal IDs.
10. **APP 10 – Quality of Personal Information**  
Ensure personal information is accurate, complete, and up to date.
11. **APP 11 – Security of Personal Information**  
Protect information from loss, misuse, or unauthorised access.
12. **APP 12 – Access to Personal Information**  
Give individuals access to their information upon request unless an exemption applies.
13. **APP 13 – Correction of Personal Information**  
Correct inaccurate or incomplete personal data promptly upon request.

### **8.3 Lawful Collection and Purpose Limitation (APPs 1, 3, 5)**

Members must collect personal information:

- Lawfully, fairly, and directly from the individual wherever possible
- Only when necessary for service provision, legal duties, or funding obligations
- With a clear explanation of:
  - Why data is being collected
  - How it will be used

- Who it may be disclosed to
- Individuals' rights to access or correct it

#### **8.4 Informed Consent and Privacy Notices (APPs 5, 6, 7)**

- Consent must be voluntary, specific, informed, and current
- Privacy notices must clearly explain:
  - What data is collected
  - Who it is shared with (including overseas disclosures)
  - How long it is stored
  - The right to opt-out of marketing or data sharing
- Marketing activities must comply with APP 7, with opt-out features provided

#### **8.5 Anonymity and Pseudonymity (APP 2)**

Where lawful and practical:

- Allow individuals to remain anonymous or use a pseudonym
- Especially relevant for general inquiries, evaluations, or surveys

#### **8.6 Secure Data Storage and Access Controls (APPs 10, 11)**

Members must implement:

- Secure systems, encrypted databases, and password protection
- Role-based access, ensuring only authorised personnel view sensitive records
- Routine data reviews to confirm accuracy and currency
- Secure disposal or de-identification when data is no longer required

#### **8.7 Cross-Border Disclosure of Information (APP 8)**

Before disclosing personal data overseas:

- Assess whether the destination country's laws provide adequate privacy protection
- Take reasonable steps to ensure the recipient complies with the APPs
- Obtain informed consent from the individual wherever necessary
- Clearly disclose offshore storage (e.g., cloud services) in privacy notices

#### **8.8 Third-Party Providers and Digital Platforms (APPs 6, 8)**

Members must:

- Use only providers who comply with Australian privacy standards

- Ensure contracts include clauses on:
  - Data protection
  - Limits on disclosure
  - Data breach procedures
- Avoid platforms that transmit data to jurisdictions with inadequate safeguards

### **8.9 Breach Response and Notifiable Data Breaches (APP 11, NDB Scheme)**

Members must:

- Maintain a Data Breach Response Plan
- Notify the OAIC and affected individuals if a breach is likely to cause serious harm
- Act quickly to contain, assess, and remediate any breach
- Inform WAFA within 72 hours of a breach involving WAFA-affiliated clients or services

### **8.10 Access and Correction (APPs 12, 13)**

Members must support individuals to:

- Access their personal information on request
- Request corrections if data is inaccurate, incomplete, or outdated
- Provide responses within a reasonable timeframe (typically within 30 days)

### **8.11 Privacy by Design and Privacy Impact Assessments**

Members must:

- Integrate **privacy protections from the outset** of any new system or project
- Conduct Privacy Impact Assessments (PIAs) when introducing new apps, platforms, or services handling personal data
- Document risks and mitigation strategies

### **8.12 Special Categories of Data – Health and Disability**

WAFA members often handle sensitive health and disability-related data. Members must:

- Collect only what is strictly necessary
- Obtain explicit consent for any sharing or disclosure
- Recognise these as ‘sensitive information’ under the Privacy Act and treat with heightened care

### **8.13 Children and Vulnerable Clients**

When services involve children, young people, or legally supported adults:

- Use age-appropriate consent procedures
- Clarify who has legal authority to consent or access data
- Implement extra safeguards to prevent coercion or misuse

#### **8.14 De-identified and Research Data**

Where identification is unnecessary:

- Use de-identified or pseudonymised data for monitoring, reporting, and research
- Ensure data cannot be reasonably re-identified
- Re-identification must never occur without lawful basis and consent

#### **8.15 Record Retention and Secure Destruction**

Members must:

- Retain records in line with legal obligations (e.g., 7 years post-service under NDIS Provider guidelines)
- Use secure methods for destruction or archiving when no longer needed
- Keep logs of disposal actions

#### **8.16 Privacy Training and Accountability**

All WAFA-affiliated staff, volunteers, and contractors must:

- Complete privacy training during induction and at regular intervals
- Be familiar with the APPs and how they apply in daily practice
- Know how to detect and report privacy breaches
- A designated Privacy Lead should oversee compliance and respond to complaints

#### **8.17 Accessible Privacy Information (APP 1)**

Privacy notices and policies must be:

- Clear, concise, and in Plain English
- Available in alternative formats, including:
  - Easy Read
  - Auslan
  - Translated languages
- Individuals must be able to ask questions or raise concerns without fear of retaliation

#### **8.18 Complaints and Escalation**

Members must provide:

- An internal complaints process for privacy concerns
- A clear path to escalate unresolved issues to:
  - WAFA, or
  - The Office of the Australian Information Commissioner (OAIC)

Members must cooperate fully with investigations and implement corrective action promptly.

### **8.19 Audit, Monitoring, and Continuous Improvement**

Members must:

- Conduct regular audits of privacy practices
- Maintain compliance evidence for WAFA review
- Document changes in policies and respond proactively to risk or complaints

## **9. Review, Revision and Approvals**

This policy will be reviewed annually by the steering committee to ensure its effectiveness and relevance. Any revisions will require approval from the steering committee.

## **10. Implementation**

WAFA members must integrate these standards into governance frameworks, operational policies, financial management, human resources, and client service delivery to maintain high standards of accountability and organisational integrity.

## **11. Enforcement**

WAFA enforces these standards through its accreditation and audit processes. Non-compliance will lead to remedial actions and may impact ongoing WAFA membership and certification status.

## **12. Contact Information**

For further information or assistance related to this standard, please contact the steering committee at the following email address: [admin@workinganimals.com.au](mailto:admin@workinganimals.com.au)

---

### Document Control

| Version | Date       | Author     | Change Description | Approved By |
|---------|------------|------------|--------------------|-------------|
| V1.0    | 17/05/2025 | V. Solomon | Initial            | C.Williams  |