Information Management Policy

Version Number	2.0
Approved by International Board	December 2022
Next Review	December 2025

World Animal Protection is a global animal protection organisation comprising a network of entities working together in furtherance of an agreed global strategy, and who all recognise the need for mutual assurance through adherence to good governance principles throughout the network.

I. Scope

1. All World Animal Protection staff, interns, volunteers (which term includes board members), and contractual third parties.
2. All World Animal Protection entities.

II. Policy

Information is a key asset for World Animal Protection, and therefore good information management is vital in serving our programme operations, in our effective and efficient functioning as an organisation, as a protection against liability, as a means of accountability to our diverse stakeholders, and in supporting our statutory compliance obligations.

This policy is designed to bring consistency to the way corporate information is created, stored, accessed and disposed of, in order to ensure the integrity of information trails in support of key initiatives, projects and relationships. It describes how World Animal Protection implements good information management, and covers information held both electronically and on paper. It should be read in conjunction with all our other global policies.

1. ### IT strategy
   1. World Animal Protection will maintain a global Information Technology (IT) strategy to support its information management policy and procedures. The strategy will have been developed by World Animal Protection International in consultation with country offices to ensure that it meets our global needs.

2. ### Information stewardship
   1. Information must be strictly managed throughout its life cycle, regardless of medium or format, for as long as it is required to meet operational and fiscal responsibilities, legal obligations, and accountabilities.

2. Information stored by the organisation will be appropriate to business requirements.

3. World Animal Protection will create appropriate systems for categorising and labelling information to facilitate its effective management. Staff are responsible for adhering to these systems.

4. World Animal Protection will systematically identify the main sources of information generated internally (including appropriate documentation of all programmatic work). We will ensure that audit trails exist relating to key decisions and that major corporate documents, including strategies, policies and procedures, are made accessible to staff, the public and regulatory authorities as required or appropriate.

5. World Animal Protection will have in place information retention and destruction procedures which will be consistent with statutory, regulatory, contractual and business requirements.

3. Information security

1. Appropriate procedures must be implemented to ensure that information is protected from a loss of:
   - Confidentiality – information will be accessible only to authorised individuals who require access to that information to fulfil their role.
   - Integrity – the accuracy and completeness of information will be maintained
   - Availability – information will be accessible to authorised users and processes when required

2. The organisation will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities.

3. The organisation's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities.

4. Information security education and training will be made available to all staff.

5. Poor and inappropriate behaviour in relation to this and related policies will be addressed through our established disciplinary processes.

6. Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

7. Information processing facilities will be housed in secure areas, physically and virtually protected from unauthorised access, damage and interference by defined security perimeters. Layered security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.

8. The organisation will ensure the correct and secure operations of information processing systems. This will include documented operating procedures; the use of formal change control, controls against malware, and vulnerability management.

9. The organisation will maintain network security controls to ensure the protection of information within its networks, and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities.

10. The organisation's information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

11. Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

12. All breaches of information security, actual or suspected, must be reported and will be investigated at a senior level, and appropriate action taken. Guidance will be available to staff on what constitutes an Information Security incident and how this should be reported.

13. Breaches of personal data must be dealt with under the Data Protection policy.

4. Information access control

1. Access to World Animal Protection's information and information systems will be driven by business requirements. Access will be granted or arrangements made for employees, partners and suppliers according to their role, only to a level that will allow them to carry out their duties.

2. A formal user registration and de-registration procedure will be maintained for access to all information systems and services.

3. Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

5. Business continuity management

1. The organisation will have in place business continuity arrangements to protect critical business processes and information from the effects of major failures of information systems or disasters and to ensure their timely resumption and retrieval respectively. These will include appropriate backup routines and built-in resilience.

2. Business continuity plans will be produced, maintained and tested for each World Animal Protection office.

6. Compliance management

1. The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements. Currently these include data protection legislation, the payment card industry data security standard (PCI-DSS), and all materials for which there may be Intellectual Property Rights, including, but not limited to, proprietary software products.

2. World Animal Protection will identify and comply with all relevant legal requirements as to the maintenance of statutory documents.

3. World Animal Protection will use a combination of internal and external audit to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures.

7. Acceptable use of information technology resources

1. Use of information technology by employees is permitted and encouraged where such use supports the goals and objectives of the business. Employees must comply with current legislation, use IT in an acceptable way, and must not create unnecessary business risk to the organisation by its misuse.

2. The organisation's expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff, and poor and inappropriate behaviour will be addressed though our standard disciplinary processes.

8. IT procurement

1. In order to ensure maintain the integrity of our systems and maximise our effectiveness, all IT purchases must be in line with World Animal Protection's global IT strategy. The Global Head of IT should be consulted if proposed IT purchases are likely to have a significant impact on, or implications for, other areas of the organisation.

2. All IT expenditure must be made with due consideration of the costs (including on-going support costs) and benefits after thorough review of all possible options, and in accordance with the Procurement provisions of World Animal Protection's Finance Policy and their corresponding protocol.

3. No additional software beyond that which is pre-approved may be purchased or installed on World Animal Protection equipment without appropriate prior agreement.