

OPERATIONAL POLICY

Use of electronic devices by authorised officers at export registered establishments

Direction to authorised officers

This document is instructional material for the Department of Agriculture and Water Resources (the department) under its Practice Statement Framework. All staff must comply with it.

Purpose of this document

This policy document provides a framework for authorised officers on the use of electronic devices and the appropriate handling of information collected by an authorised officer.

In this document

This document contains the following topics.

Purpose of this document	1
Definitions	2
Policy statement	2
Objective of this policy	2
Legislative framework	3
Roles and responsibilities	3
The department's commitment	3
Implementation	3
Ongoing verification	3
Background	3
Contact Information	
Policy	
Suitable electronic devices for photographic or videographic evidence	
Rules for collecting evidence	4
Use of personal electronic devices	4
Ownership of evidence	5
Related material	5
Document information	5
Version history	5

This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the IML version prior to use.

Version Number: 2.0 1 of 5

Definitions

The following table defines terms used in this document.

Term	Definition
Area Technical Manager (ATM)	Department veterinary officers who are responsible for the overall supervision of the On-Plant Management System and authorised officers at export registered slaughtering establishments/ independent boning rooms in a defined geographical location.
Authorised officer	Means a person appointed by the Secretary under section 20 of the <i>Export Control Act</i> 1982 to exercise or perform all or some of the powers or functions of an authorised officer under this Act or of such of those powers as are specified in the instrument.
Breach	A critical non-compliant issue where it is reasonably possible that the evidence could be used in a prosecution.
Electronic device	A mobile phone, tablet, iPad, camera or any other portable device capable of electronically or digitally recording audio and/or video.
Establishment	Means an establishment, including premises, that is registered in respect of the operations for the preparation of meat and meat products for export for food under clause 5 of Schedule 1 of the <i>Export Control (Meat and Meat Products) Orders</i> and which has an approved arrangement in accordance with Order 30 of those Orders.
Supervisor	A senior department officer in the department's relevant organisational structure who is responsible for managing performance of the authorised officer.

Policy statement

Electronic devices are issued to department staff to support communication between themselves, their supervisors and management.

Department staff regulating export meat legislation, may be required to use these department-issued devices to record information to support State, Territory and Commonwealth legislative and market access requirements.

Electronic devices used to record evidence must be:

- fit for purpose; and
- up to date

Date published: 27/06/2018

to securely record, handle and maintain sensitive digital information.

Objective of this policy

Ensure authorised officers are aware of their obligations to securely record, handle and maintain sensitive digital information as evidence in cases where the company does not discharge its obligations properly.

Management of recorded breaches is not within the scope of this policy.

This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the IML version prior to use.

Use of electronic devices by on plant officers at export registered establishments

Legislative framework

The following list outlines the legislation that applies to authorised officers exercising their powers to take photographs or make audio or video recordings as part of evidence collection:

Export Control Act 1982 - Clauses 10 and 11L

Criminal Code Act 1995 - Section 149.1

Roles and responsibilities

The following table outlines the roles and responsibilities of departmental officers under this departmental policy.

Role	Responsibility
authorised officer	 must comply with this policy. may collect evidence in cases where the company doesn't discharge its obligations properly ensure that the device is in their physical control at all times.
supervisor	 ensure the authorised officers they supervise are provided this policy verify that the authorised officers they supervise comply with this policy at all times.

The department's commitment

The department will ensure accurate and secure records by:

- ensuring that authorised officers are aware of their responsibilities
- providing suitable training
- issuing and maintaining suitable electronic devices to on plant staff.

Implementation

The service delivery group will:

- implement a process that facilitates awareness and obligations of collecting evidence, such as adequacy of electronic devices to meet current evidence collection requirements
- assign a suitable device to each export registered meat processing establishment for OPV use.

Ongoing verification

The Export Meat Program will:

• undertake verification activities to ensure this policy is complied with.

Background

Export meat establishments generally have a prohibition on their staff and visitors using cameras on site. However the <u>Export Control Act (1982)</u> permits the use of cameras by authorised officers under certain, restricted conditions.

Under Clause 10 of the <u>Export Control Act (1982)</u>, the powers an authorised officer may exercise in relation to particular premises include the "taking of photographs (including video and audio recordings)" for the purposes of evidence collection.

This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the IML version prior to use.

Date published: 27/06/2018 3 of 5

Version no.: 2.0

Contact Information

Contact: Enforcement Section in your nearest regional office

Should authorised officers have any questions or are seeking advice please do not hesitate to contact the Enforcement Section. The Enforcement Section staff are available to meet with onsite vets to provide guidance if needed.

Policy

Suitable electronic devices for photographic or videographic evidence

The device must be able to:

- record evidence of breaches of conduct in relation to export legislative requirements
- retain the integrity of the evidence securely
- accurately note the time and date the evidence was recorded
- record videographic evidence where required
- transfer content to a department on-plant computer for further action
- be 'locked' with a password, when not in use.

Rules for collecting evidence

An authorised officer must:

- only use department-issued cameras or other electronic devices to support the role of the authorised officer
- comply with the Australian Public Service (APS) Code of Conduct at all times
- record reliable and secure note of the breach at the time of occurrence, or shortly thereafter
- inform the establishment management that evidence of the breach will be collected, or shortly thereafter and providing information on the evidence that was collected
- carefully handle and maintain the physical integrity of the evidence collected to preserve information
- · must securely manage the chain of custody of evidence (i.e. immediate and direct transfer of evidence to the department network then immediately delete permanently from the portable electronic device)
- ensure that digital image(s) provide sufficient detail to support evidence
- not share a portable electronic device with an unauthorised person.
- not connect any personally owned electronic device directly to the department's network, as per the department's IT policy.

Use of personal electronic devices

In exeptional circumstances, a personal device may be used to collect evidence where:

- the department issued device cannot be used, and
- there is no other viable option available, and
- an authorised officer determines that evidence may be lost imminently.

If this has been the case, the authorised officer must:

- apply the above rules for collecting evidence
- contact the Enforcement Section for advice on the management of the evidence
- not connect their personal electronic device to any personally-owned electronic information storage or retrieval systems (i.e. cloud, personal file sharing network, other personal device).

This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the IML version prior to use.

Version no.: 2.0 Date published: 27/06/2018 4 of 5

Ownership of evidence

Evidence recorded by an authorised officer is:

- the property of the Australian Government at all times
- not considered to belong to the authorised officer who collected the evidence
- considered commercial-in-confidence: sensitive and must not be transmitted, uploaded, copied
 or disseminated to unauthorised third parties or copied to the photographer's own storage
 devices. Any leaking of information will be dealt with in line with the department's Protective Security Plan.
- retained securely prior to being legally destroyed in line with department <u>records authorities</u> once it has reached its use by date.

Related material

- Legislation: Australian Public Service 1999 Code of Conduct
- Legislation: Export Control Act 1982
- Legislation: <u>Criminal Control Act 1995</u>
- Policy: <u>Protective Security Plan</u> (Note: Access only available using the department network)
- Policy: <u>Department IT Security</u> (Note: Access only available using the department network)
- Policy: Records Authorities (Note: Access only available using the department network)
- <u>Learnhub</u>: Regulatory officer note taking
- Learnhub: Evidence Handling

Document information

The following table contains administrative metadata.

Instructional material owner:	Assistant Secretary, Meat Exports Branch
Instructional Material Library document ID:	External publication
Freedom of information exemption:	No
TRIM container number:	2017/008653E
Review date:	June 2021

Version history

The following table details the published date and amendment details for this document.

Version	Date	Amendment details
1.0	05/06/2017	 First publication of this policy on the department website. Incorporating all types of electronic portable devices to record evidence.
2.0	27/06/2018	Reviewed and agreed to review in 3 years.

This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the IML version prior to use.

Version no.: 2.0

Date published: 27/06/2018 5 of 5