DOC 2

GENERAL ORDER
DIGITAL INFORMATION MANAGEMENT FRAMEWORK

General Order title	**Digital information management framework**
Date of issue	4 October 2023
Date of operation	27 September 2023
Review date	September 2026
Review responsibility	Metropolitan Operations Service Executive
Replaces	Previous General Order, **Digital information management framework**
PCO reference	2016/0943
Gazette reference	SAPG 188/23
Enquiries to	Operations Support Coordinator Telephone 732 24505
Corporate Policy Sponsor	Assistant Commissioner Metropolitan Operations Service

General Orders provide an employee with instructions to ensure organisational standards are maintained consistent with SAPOL's vision. To this end, General Orders are issued to assist an employee to effectively and efficiently perform their duties. It is important that an employee constantly bears in mind that the extent of their compliance with General Orders may have legal consequences.

Most orders, as is indicated by the form in which they are expressed, are mandatory and must be followed. However, not all situations encountered by an employee can be managed without some form of guidance and so some of these orders are prepared as guidelines, which should be applied using reason. An appendix to a General Order will be regarded as part of the General Order to which it relates. At all times an employee is expected to act ethically and with integrity and to be in a position to explain their actions. Deviation from these orders without justification may attract disciplinary action.

To ensure best practice an employee should be conversant with the contents of General Orders.

The contents of General Orders must not be divulged to any person not officially connected with SAPOL. Requests for General Orders will be managed as follows:

- Civil subpoena and disclosure requests—contact the Information Release Unit.
- Criminal subpoena and disclosure requests—refer to General Order, **Disclosure compliance and subpoena management**.
- Freedom of information requests—contact the Freedom of Information Unit.
- Any other requests (including requests by employees)—refer to instructions provided within General Order, **Corporate policy framework**, **5. GENERAL ORDER REQUESTS/RELEASE**.

CONTENTS

1. GENERAL ORDER STATEMENT

In the constantly changing digital environment it is critical to provide an overarching framework to manage digital information. South Australia Police (SAPOL) aims to safely and efficiently manage all property in its custody including digital information. Management includes the manner, methods and processes of dealing with the information including how it is captured, collected, recorded, retained, retrieved and/or destroyed.

This General Order contains principles and governing instructions concerning the management of digital information obtained through the use of all digital recording devices (DRDs). This includes DRDs provided by either SAPOL or otherwise (including privately owned) where they are used by SAPOL employees. The principles provide overarching requirements and considerations, and the governing instructions provide specific operational requirements.

Any policy regarding digital information or devices must be in accordance with the principles and governing instructions within this General Order and include them as the foundation for a policy.

Scope

This General Order applies to all employees of SAPOL.

2. PRINCIPLES FOR THE MANAGEMENT OF DIGITAL INFORMATION

SAPOL supports the use of DRDs for the capture of digital information providing the use of these devices contributes to achieving SAPOL's core functions. Using devices to capture incidents, events and interactions with members of the public must be balanced against community expectation and their right to conduct or engage in lawful activities.

SAPOL's use, storage and management of digital information, regardless of value, should comply with the following principles.

Provision of equipment

SAPOL provides equipment, systems and technology for dealing with lawfully collected digital information including how it is captured, collected, recorded, retained, retrieved and/or destroyed. The use of devices and policies regarding digital information must comply with the *Work Health and Safety Act 2012*.

Non-SAPOL digital recording devices

SAPOL permits, but does not encourage, the use of non-SAPOL DRDs and may not provide technical support for such use. When an employee chooses to use a non-SAPOL DRD they accept responsibility for the information captured, including collection, storage, security, disclosure, destruction, and compliance with policy and legal obligations. SAPOL may assist when the copying and storage of information is required for evidentiary purposes.

Device specific policies and standard operating procedures

Each SAPOL DRD will have an approved operating policy. The policy will provide operational direction and guidance, for the use and management of devices, and information.

Ownership of digital evidence/information

Any digital evidence/information captured by SAPOL employees whilst on duty is the property of SAPOL and must be managed according to General Orders, policy and legislative requirements.

Information captured will not be transferred or used other than for the lawful discharge of police duties, or for any other purpose without the specific approval of an employee's officer in charge, being a substantive officer of police (of or above the rank of inspector). In exceptional circumstances where an employee's officer in charge is not available, approval may be sought from another substantive officer of police.

Legislative requirements

The use of DRDs must comply with legislative and investigational procedures. Any digital evidence/information captured by these devices must be managed in accordance with the rules of evidence including the requirements of disclosure. The use of these devices should not be used as a replacement for the accepted evidence of police observations and the documentation (notes) of these observations.

Ethical considerations

Policies for all DRDs will give consideration to the balance between ethical and professional judgement and discretion of the circumstances to the legislative requirements, and potential loss of best evidence. In some circumstances it may be more appropriate to use traditional methods of obtaining information.

Collection

Only digital information which is relevant to an investigation or for the purpose of approved SAPOL training will be collected, captured, stored and/or retained. Such collection, capture, storage and/or retention will be in compliance with SAPOL instructions and legislative requirements.

4(2)(a)(vi) and 4(2)(b)

Digital Asset Management system for public submission

SAPOL have implemented a technology based solution to receive photos and videos which may have been captured on mobile phone, closed circuit television (CCTV) or dash-camera relating to significant incidents or investigations. The system is a Digital Asset Management (DAM) 7(1)(c)

Photos and videos are uploaded by members of the community 4(2)(a)(vi) and 4(2)(b) 4(2)(a)(vi) and 4(2)(b) which SAPOL can access, review and assess to ensure relevant information or evidence is obtained at the earliest opportunity. This is the preferred methodology to capture digital information.

A select number of members across Metropolitan Operations Service (including Crime Coordination Section and Intelligence areas), Crime Service, State Crime Assessment Centre and Investigation Support Desk have been trained to review and manage the submission of footage via 7(1)(c)

Public appeal process

The requesting investigating officer must liaise with their local trained 7(1)(c) user who will create a portal for public appeals. After a portal is created, both a link and QR code are generated directing the member of the public (MOP) to the 7(1)(c) . The MOP selects 'submit evidence' allowing them to nominate an email address or telephone number. An individual link is automatically sent to the MOP (via their preferred contact method) for them to upload the information to the 7(1)(c) portal.

An 7(1)(c) user will then review the information and either accept or decline it based on evidential value. Any evidence obtained will be downloaded by the 7(1)(c) user and dealt with as per police property management procedures (refer to General Order, **Property**). All information/evidence received or downloaded is digitally timestamped for chain of evidence purposes and can be obtained from the 7(1)(c) portal.

Individual requests

The most common are individual requests for information which are a separate process to public appeals. This is where evidence of value is already known to exist and police have already liaised with a member of the public or business. An 7(1)(c) user provides an email or SMS to the MOP (or business), for them to upload any information. The information is reviewed by the 7(1)(c) user and where evidence is obtained, it will be downloaded (by the 7(1)(c) user) and processed as per police property management procedures (refer to General Order, **Property**). The investigating officer will then receive a notification to review all information and/or evidence provided.

The 7(1)(c) contains information and help pages to assist users.

7(1)(c) may be used to view and download images and CCTV for investigations. Video footage and images may be retrieved from the 'evidence locker' section. This platform is securely encrypted and enables the efficient transfer of evidence between retailers and police. Further information regarding this process is contained within the Standard Operating Procedure—7(1)(c)

Crime Stoppers enables members of the public to submit digital information and remains the preferred method to be used for general public appeals for assistance.

The collection of taxi CCTV by investigators is outside the DAM system and Crime Stoppers process.

Storage and destruction

The storage and/or destruction of all digital information collected/captured must comply with legislation, SAPOL policy and State Records of SA General Disposal Schedule 30 (GDS 30).

3. GOVERNING INSTRUCTIONS

The following instructions must be read in conjunction with **2. PRINCIPLES FOR THE MANAGEMENT OF DIGITAL INFORMATION** previous in this General Order. These instructions apply to both SAPOL and non-SAPOL DRDs unless specifically stated.

Use

Non-SAPOL DRDs will not be used in preference to SAPOL approved devices. Employees are under no obligation to utilise a non-SAPOL DRD when SAPOL equipment fails or is not available.

Employees must only make a digital recording of interactions with the public in the normal course of their duties and only for a specific policing duty.

A specific policing duty is defined as a specific interaction with the public which occurs in the course of an employee's duty. This may include a traffic stop or tasking, but does not include interactions with colleagues, supervisors or managers, or in any other environment which is not considered a specific policing duty.

Management

Where DRDs have been used to capture and record interactions with the public, the recordings may not initially fall into any category that requires the data or information to be retained for legislative or evidentiary purposes. However, it may provide an accurate record of an interaction with the public which may be subject to a criminal or internal investigation and/or proceeding.

At the time an employee becomes aware of the value of the record (where the record is still available) they must treat any information captured as an exhibit by extracting the data and entering the data as an exhibit as per General Order, **Property** and the Property management manual.

Any digital information captured in the course of an employee's duties (which may be seen as an extension of notes made by an employee) must be captured, stored, retained, retrieved and/or destroyed in compliance with legislation and SAPOL policy. This includes compliance with the *State Records Act 1997* through the Operational records disposal schedule—SAPOL, which provides timelines for the retention of information. **This includes any recording under legislative requirements and/or that has an evidentiary value**.

Any digital information captured on a DRD must not be further distributed (such as through media, social media or by other means) without express approval as defined at **2. PRINCIPLES FOR THE MANAGEMENT OF DIGITAL INFORMATION, Ownership of digital evidence/information** previous in this General Order.

For the purposes described in this instruction, employees may connect non-SAPOL DRDs to SAPOL computers. Some devices and non-standard formats will not be supported and in these circumstances, where the content is required to be retained for evidentiary purposes, the copy and storage should be referred to Digital Evidence Section for specialist assistance. Employees must refer to Information Systems and Technology (IS&T) Service requirements in General Orders and/or policy when connecting non-SAPOL DRDs to SAPOL systems.

A list of current software and hardware standards which are supported by SAPOL are available through the intranet.

Safety

At no time will an employee use any DRD which is in contravention of the intended use of that device.

Regardless of whether an employee is using a SAPOL or a non-SAPOL DRD, employees will not use the device in any manner which would or may place the safety of themselves or others in jeopardy.

At no time will an employee interfere with the function, access or safety standards of any SAPOL equipment or vehicle. Use of any equipment, either supplied by SAPOL or otherwise, must be in compliance with the *Work Health Safety Act 2012* and General Order, **Work health, safety, wellbeing and injury management**.

Dress standards

Employees who use or wear a non-SAPOL DRD must ensure it complies with General Order, **Dress standards** and General Order, **Operational safety—operational equipment**. Supervisors are responsible for monitoring and assessing the wearing of these devices and must ensure compliance with General Orders and the professional dress standards expected by SAPOL and the community are maintained.

4. REFERENCES

General Disposal Schedule 30

General Order 8185, **Business management, Asset management, Asset register and monitored items**

General Order 8185, **Business management, Information management, Disposal of records**

General Order 8450, **Information technology management, Computer equipment management**

General Order 8450, **Information technology management, Information and communication technology governance**

General Order 8450, **Information technology management, Information security**

General Order 8450, **Information technology management, Portable computing and data storage**

General Order, **Body worn video and VideoManager**

General Order, **Dress standards**

General Order, **Information—access and release**

General Order, **Operational safety**

General Order, **Operational safety—operational equipment**

General Order, **Property**

General Order, **Purchase, use and disposal of items and equipment**

General Order, **Records management**

Property management manual

SAPOL 2030

Standard Operating Procedure—7(1)(c) .

Operational records disposal schedule—SAPOL

South Australia Police Digital Strategy 2022-24

State Records Act 1997

Work Health and Safety Act 2012

5. FURTHER ENQUIRIES

Operations Support Coordinator, Metropolitan Operations Service, telephone 732 24505.

6. DOCUMENT HISTORY SINCE 26/10/2016

Gazette reference (SAPG)	Date	Action (amendment/deletion/new/review/temporary variation)
226/16	26/10/16	New General Order.
49/20	11/03/20	Review 2020—including being renamed to Digital information management framework.
188/23	04/10/23	Review 2023—at **2. PRINCIPLES FOR MANAGEMENT OF DIGITAL INFORMATION**: **Collection** malware content added and new subheadings **Digital Asset Management system for public submission, Public appeal process** and **Individual requests**. Content added concerning 7(1)(c) and 7(1)(c) processes. All references to uwitnessit have been deleted.

APPROVED BY COMMISSIONER/DEPUTY

…… *Print Full Name*

…… *ID Number*

…… *Signature*

27/09/2023 *Date*

Documentation certification and verification

General Order draft prepared by: Sergeant Craig Terlikowski, Metropolitan Operations Service

General Order updated by: Detective Senior Sergeant Allan Grimwood, Acting Planning and Audit Officer, Metropolitan Operations Service
General Order verified by: Assistant Commissioner Scott Duval, Metropolitan Operations Service