



OFFICIAL: Sensitive

## GENERAL ORDER INFORMATION—ACCESS AND RELEASE

<b>General Order title</b>	<b>Information—access and release</b>
<b>Date of issue</b>	22 September 2021
<b>Date of operation</b>	8 September 2021
<b>Review date</b>	August 2024
<b>Review responsibility</b>	Information Services Branch
<b>Replaces</b>	Previous General Order, <b>Information—access and release</b>
<b>PCO reference</b>	13/02745–02
<b>Gazette reference</b>	SAPG 182/21
<b>Enquiries to</b>	Manager, Information Services Branch Telephone 732 23455
<b>Corporate Policy Sponsor</b>	Director, Business 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

<b>1. GENERAL ORDER STATEMENT</b> .....	<b>4</b>
<b>Scope</b> .....	<b>4</b>
<b>2. DEFINITIONS</b> .....	<b>4</b>
<b>3. LEGISLATION</b> .....	<b>4</b>
<b>Police Complaints and Discipline Regulations 2017</b> .....	<b>4</b>
<b>Code of Ethics for the South Australian Public Sector</b> .....	<b>5</b>
<b>Public Sector (Data Sharing) Act 2016</b> .....	<b>5</b>
<b>4. ACCESS AND RELEASE FRAMEWORK</b> .....	<b>5</b>
<b>5. SA GOVERNMENT GUIDELINES</b> .....	<b>5</b>
<b>Information privacy principles</b> .....	<b>6</b>
<i>Disclosure of personal information</i> .....	<b>6</b>
<b>Personal information data breaches guideline</b> .....	<b>7</b>
<b>Information sharing guidelines</b> .....	<b>7</b>
<b>Interagency code of practice</b> .....	<b>8</b>
<i>Child abuse by school employees</i> .....	<b>9</b>
<b>6. ADMINISTRATIVE RELEASE</b> .....	<b>9</b>
<b>Subpoenas/disclosure requests</b> .....	<b>9</b>
<i>Civil jurisdiction</i> .....	<b>9</b>
<i>Criminal jurisdiction</i> .....	<b>9</b>
<b>Release of police reports</b> .....	<b>9</b>
<i>Occurrence report</i> .....	<b>9</b>
<i>Vehicle collision report</i> .....	<b>10</b>
<b>Criminal records</b> .....	<b>10</b>
<b>National police certificate</b> .....	<b>10</b>
<b>Freedom of Information Act 1991</b> .....	<b>10</b>
4(2)(a)(iv) and 4(2)(b) 	
<b>Blood/breath analysis certificates</b> .....	<b>13</b>

**7. OPERATIONAL RELEASE ..... 13**

**Child abuse reporting line..... 13**

4(2)(a)(iv) and 4(2)(b)

**Community safety..... 13**

**Intelligence ..... 14**

**Joint agency operations..... 14**

**Listening and surveillance devices..... 14**

4(2)(a)(iv) and 4(2)(b)

**Telecommunications interception..... 14**

**Media..... 15**

**Solicitor interviews ..... 15**

**Victims ..... 15**

**8. INFORMATION AND COMMUNICATIONS TECHNOLOGY ..... 15**

**9. CRIME STATISTICS AND ORGANISATIONAL PERFORMANCE**

**DATA..... 15**

**Corporate level data ..... 15**

**District/LSA/branch data ..... 16**

**Collating data ..... 16**

**10. MASKING OF SAPOL RECORDS..... 16**

**Masking PIMS records..... 16**

*Access to PIMS masked records..... 17*

**Masking Shield records..... 17**

*Access to Shield masked records..... 17*

**11. REFERENCES ..... 17**

**12. FURTHER ENQUIRIES ..... 18**

**13. DOCUMENT HISTORY SINCE 18/11/2009 ..... 18**

## 1. GENERAL ORDER STATEMENT

The purpose of this General Order is to identify employee responsibilities in relation to the access and release of South Australia Police (SAPOL) information.

An employee must not release information in contravention of General Orders, legislation or policy frameworks.

### Scope

This General Order applies to all SAPOL employees, contractors and organisations working for and on behalf of SAPOL.

## 2. DEFINITIONS

For the purpose of this General Order the following definitions apply.

**Access**—directly or indirectly obtaining knowledge or possession of official information contained in a document, record or computer system.

**Administrative release**—the formal release of official information to persons, agencies or organisations external to SAPOL, in line with statutory, court ordered, or policy frameworks. Refer to **6. ADMINISTRATIVE RELEASE** further in this General Order.

**Intelligence holdings**—all products and systems under governance, control or oversight of State Intelligence Branch (SIB) including physical documents, electronic records, street checks and intelligence submissions, material created, produced or stored in accordance with the Intelligence business process (IBP), or other relevant policies. All intelligence holdings are considered to be 'held' by SIB, whether in actual possession of SIB or not.

**Official information**—any information generated or held by SAPOL that is not publicly available including intelligence holdings, sensitive information and security classified information.

**Operational release**—the release of official information by an employee in the course of an investigation, operation, or during the management of an incident, including any subsequent prosecution or coronial process. Refer to **7. OPERATIONAL RELEASE** further in this General Order.

**Release**—directly or indirectly communicating, transmitting, publishing or otherwise disseminating official information, including verbal, electronic or paper based release.

**Security classified information**—official information that has been assigned a security classification such as 'protected', 'secret' or 'top secret'.

## 3. LEGISLATION

### Police Complaints and Discipline Regulations 2017

Schedule 3 clause 10 of the Police Complaints and Discipline Regulations 2017 states:

A designated officer must treat information obtained by SA Police (or by the designated officer by virtue of his or her employment) as confidential and must not –

- (a) seek to obtain access to such information except in the proper execution of his or her duties; or

- (b) improperly use or disclose such information.

### **Code of Ethics for the South Australian Public Sector**

Public sector employees will not access or attempt to access official information other than in connection with their duties or as authorised.

Public sector employees will not disclose official information acquired through the course of their employment other than is required by law or as appropriately authorised in the agency concerned.

### **Public Sector (Data Sharing) Act 2016**

SAPOL is bound by the *Public Sector (Data Sharing) Act 2016*, which provides a safe, legal framework to share public sector data between government departments and other trusted entities.

## **4. ACCESS AND RELEASE FRAMEWORK**

The following framework must be followed by employees who access and release official information:

- all employees are responsible for maintaining the security and confidentiality of official information
- official information must be stored, handled and managed in accordance with any security classification marking, dissemination limiting marking or other caveat attached to the information
- employees must not access or release official information except in the lawful execution of their duties
- official information must only be released to persons who have been appropriately identified and have demonstrated a lawful reason to receive the information
- official information should not be released where it is likely to compromise an investigation, operation or prosecution
- when an employee suspects that release of official information would be likely to compromise an investigation, operation or prosecution they must not release the information unless the release is authorised by the officer in charge/manager of the area responsible for the investigation, operation or prosecution
- classified information must only be released to persons who have the appropriate level of clearance and a genuine need to know the contents of the classified information.

In addition to the authorities identified in this General Order, official information may be authorised for release by the Commissioner of Police, the Deputy Commissioner or the Executive Leadership Team (ELT) member responsible for the information concerned.

## **5. SA GOVERNMENT GUIDELINES**

SAPOL supports a collaborative interagency approach to managing the administrative and operational release of official information. A number of principles and protocols are relevant when employees consider releasing information.

## Information privacy principles

The *Information Privacy Principles* (IPPs) form a Cabinet Administrative Instruction (PCO12) applying to all South Australian Government agencies. The IPPs regulate the way agencies collect, use, store and disclose personal information. The IPPs are administered by the Privacy Committee of South Australia.

Chief Executives are responsible for ensuring the principles are implemented, maintained and observed for and in respect of all personal information for which their agency is responsible.

### *Disclosure of personal information*

Clause 10—Disclosure of personal information of the IPPs restricts the release of personal information as follows:

- (10) An agency should not disclose personal information about some other person to a third person unless:
  - (a) the record-subject would reasonably expect the agency to disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose of collection;
  - (b) the record-subject has expressly or impliedly consented to the disclosure;
  - (c) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person;
  - (d) the disclosure is required or authorised by or under law;
  - (e) the disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer;
  - (f) the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
  - (g) the agency reasonably believes that the disclosure relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and
  - (i) the agency reasonably believes that the disclosure is appropriate in the circumstances; and
  - (ii) the disclosure complies with any guidelines issued by the Minister for the purposes of this clause.

An employee is authorised to release information in accordance with the PCO12 IPPs, available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup> [REDACTED]

These principles apply to the release of official information whether for administrative or operational purposes.

## Personal information data breaches guideline

The *Personal information data breaches guideline* has been developed to provide advice to South Australian Government agencies regarding the identification and notification of inappropriate disclosure of personal information held by their agency.

A personal information data breach occurs when official information that is not already publicly available, is lost or subjected to unauthorised access, use, modification, disclosure or misuse. Personal information data breaches may occur in a number of ways, including accidental loss, internal errors or deliberate actions of trusted employees, theft of physical assets or the theft or misuse of electronic information (for example a cyber-attack).

The *Personal information data breaches guideline*, outlining how agencies should manage, process and who to notify when a data breach occurs, is available through the Internet at <[https://dpc.sa.gov.au/\\_\\_data/assets/pdf\\_file/0009/47394/Personal-Information-Data-Breaches.pdf](https://dpc.sa.gov.au/__data/assets/pdf_file/0009/47394/Personal-Information-Data-Breaches.pdf)>.

## Information sharing guidelines

The *Information Sharing Guidelines for Promoting Safety and Wellbeing* (ISGs) were approved by Cabinet as a state-wide process for information sharing to improve service coordination wherever there are threats to safety and wellbeing. They aim to support all vulnerable people, including children, young people and all adults irrespective of their status as a parent or caregiver. The ISGs are designed to give service providers confidence in sharing information appropriately with each other in order to respond or prevent harm.

The ISGs were developed by an interagency committee (which included SAPOL) and are mandated by SA Government and administered by the Department of the Premier and Cabinet.

The ISGs facilitate the release of information by employees and are available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup> [redacted]

The ISGs do not require separate record keeping systems. Employees are expected to use existing SAPOL record management procedures to record information sharing decisions as part of their every-day work with the community, colleagues, supervisors or line managers.

Record keeping requirements are outlined in the table below. Although the ISGs seek to maintain records of approval for sharing without consent, the Ombudsman acknowledges this is neither practical nor reasonable in a policing context and accepts the interrelated role of decision-making and policing as it relates to the ISGs.

Information is shared with consent (by you or to you)	Information is shared without consent (by you or to you)	Information sharing request is refused (by you or to you)
<ul style="list-style-type: none"> <li>• who gave it, when and to whom</li> <li>• what the consent related to</li> <li>• information sought, provided or received</li> <li>• outcomes and follow ups</li> </ul>	<ul style="list-style-type: none"> <li>• why obtaining consent was unreasonable or impracticable</li> <li>• your line manager's approval</li> <li>• what is shared, when and by whom</li> <li>• the agency and the office or officer involved (receiving and providing)</li> <li>• outcomes and follow ups</li> </ul>	<ul style="list-style-type: none"> <li>• the purpose (the immediate or anticipated risk the request was intended to address)</li> <li>• reason given for refusal</li> <li>• your line manager's approval</li> <li>• outcomes and follow up</li> </ul>

In all circumstances
<p><b>Make a record outlining:</b></p> <ul style="list-style-type: none"> <li>• consent (yes or no)</li> <li>• the information shared</li> <li>• who information is shared with</li> <li>• why information is shared—for what purpose/what is the risk of harm</li> <li>• what is the outcome—for example undertakings and follow up action by each party.</li> </ul> <p><b>Other considerations:</b></p> <ul style="list-style-type: none"> <li>• Notes need to be kept in Service-related electronic or hard file systems (as opposed to personal file systems) so that the information ‘follows’ the incident/person.</li> <li>• Systems should be secure, for example lockable hard files or limited access/password protected electronic files.</li> <li>• Appropriate record systems—for example Shield.</li> <li>• If unsure where to store records in your work situation, a line manager should be asked.</li> <li>• Be factual and record only what is relevant to the purpose.</li> <li>• Identify the people whose actions or views are being recording, for example “Sue Smith, youth worker at Second Story, provided...”</li> <li>• State when recording opinion or hearsay, for example, “It was Sue Smith’s view that ...”</li> <li>• Be respectful and specific in noting an individual’s problems, for example, “Offender demonstrates very concerning behaviours and is incoherent” rather than, “he is either off with the fairies or smashed.”</li> <li>• Note the details and reasons of the supervisor, officer in charge or manager approving disclosure without consent or refusal to share information.</li> <li>• Ensure notes are dated (include day, month and year) and signed (or attributable to a staff member if electronic).</li> </ul>

In accordance with the ISGs requirements SAPOL has developed an ISG appendix (procedure) to provide specific operational guidance. The *South Australia Police (SAPOL) ISG Appendix (procedure)* includes a two page flow chart (the ISGs decision making steps and practice guide). This is the state-wide process used by government agencies and non-government organisations when making information sharing decisions, available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup> [redacted]

**Interagency code of practice**

The *Interagency Code of Practice for Investigation of Suspected Child Abuse or Neglect (ICP)* describes how agencies and organisations investigate suspicion of child abuse and neglect. The ICP’s purpose is to provide, in one document, the key actions practitioners and investigators are involved in for an investigative response to suspected child abuse or neglect. The document was endorsed by the respective agency heads including the Commissioner of Police and a number of non-government organisations and associations.

An employee is authorised to release information in accordance with the ICP, which is available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup> [redacted]

The ICP applies to the release of official information for operational purposes only.

### *Child abuse by school employees*

The *ICP Appendix C: Issues specific to the education sector* deals with the investigation of offences involving child abuse by an education sector employee, service provider or volunteer. The investigating officer or supervisor will contact the relevant education sector to discuss the best course of action, and in the case of early childhood and out of school hours care sector, the Education and Early Childhood Standards and Registration Board.

## **6. ADMINISTRATIVE RELEASE**

An employee must not access or release official information for administrative purposes without authorisation.

Administrative purposes means the formal release of official information to persons, agencies or organisations external to SAPOL and includes criminal records, national police certificates, statistics, et cetera and includes statutory notifications (for example Teachers Board) and release under the *Freedom of Information Act 1991*.

Except in urgent circumstances, official information released for administrative purposes should not be released verbally. In accordance with the ISGs, a record needs to be kept of what was released, to whom it was released, and the authority for the release.

Information Services Branch (INSB) has the Commissioner of Police's delegated authority to provision the administrative release of information on behalf of SAPOL.

### **Subpoenas/disclosure requests**

An employee must not directly release information in response to a subpoena or disclosure request. Requests must be directed to the appropriate area depending on the jurisdiction of the relevant court. Refer to General Order, **Disclosure compliance and subpoena management**.

#### *Civil jurisdiction*

All subpoenas or disclosure requests relating to matters in the civil courts must be forwarded to the Manager, Information Release Unit, INSB who will determine whether there is authority to release the information.

#### *Criminal jurisdiction*

Refer to General Order, **Disclosure compliance and subpoena management**.

### **Release of police reports**

INSB is authorised to release copies of police reports made to SAPOL by members of the public. All requests should be submitted by email to 4(2)(a)(vi) and 4(2)(b)

#### *Occurrence report*

A member of the public who is a victim of a crime may obtain a copy of an occurrence report for insurance purposes by completing a **PD268 Application for report relating to a crash, theft or stolen property (PD268)**.

### *Vehicle collision report*

When the driver of a vehicle involved in a collision does not obtain the details of another party involved in the collision because of a legitimate reason (for example hospitalisation or arrest), they may be provided with the information which is included on the motor vehicle collision report.

A member of the public involved in a vehicle collision or a public utility, local government body or any other organisation may obtain a copy of a motor vehicle collision report where they are an interested party for insurance/litigation purposes by completing a **PD268**.

Employees receiving the **PD268** must obtain payment of the fee (refer to General Order, **Rates—service fees**) and conduct a 100 point verification of the person. The **PD268** should be dispatched to the Information Release Unit (internal postcode 104) the same day it is received.

### **Criminal records**

A member of the public may obtain a copy of their criminal record by completing a **PD360 Application for access to SAPOL records (PD360)**. The completed **PD360** should be forwarded to the Manager, Freedom of Information Unit. Refer to General Order, **Freedom of information**.

### **National police certificate**

A member of the public may apply for a national police certificate which provides disclosable court outcomes and pending charges (pursuant to the *Spent Convictions Act 2009*). This certificate is generally required when the applicant is seeking employment or volunteering with an agency, or for visa/licensing purposes.

The applicant must complete a **PD267 National police check application (PD267)**. Employees receiving the **PD267** must obtain payment of the fee (refer to General Order, **Rates—service fees**) and conduct a 100 point verification of the person. The **PD267** should be dispatched to the Information Release Unit (internal postcode 104) the same day it is received.

Alternatively, a National criminal history record check may be obtained through an Australian Crime Intelligence Commission approved and accredited agency.

When the purpose for a certificate is working with children the applicant is to be directed to Department of Human Services.

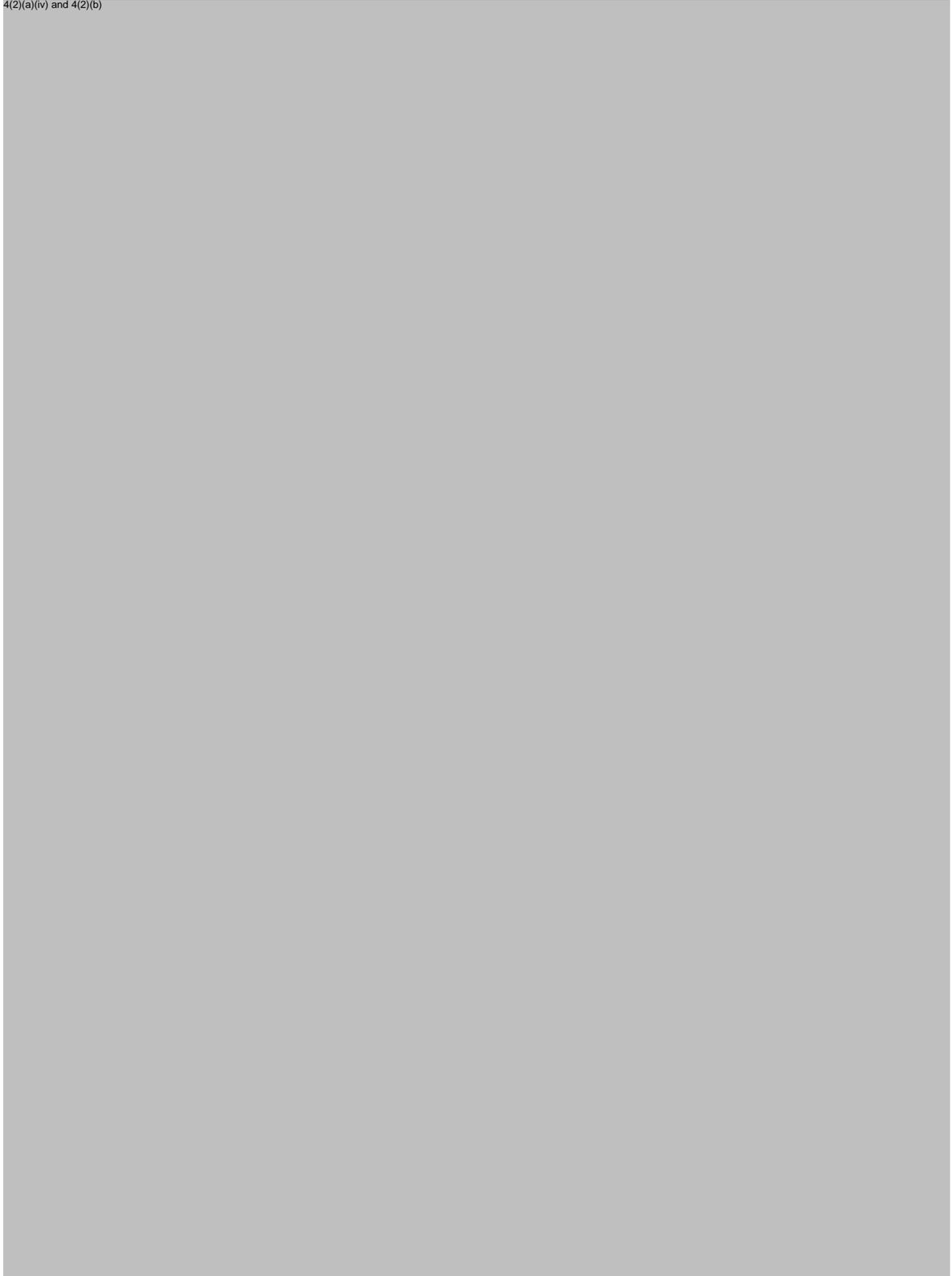
### **Freedom of Information Act 1991**

All requests for the release of documents/information not otherwise authorised by law or General Orders should be forwarded to the Manager, Freedom of Information Unit. The applicant should complete a **PD360** and pay the application fee in accordance with the *Freedom of Information Act 1991*. Refer to General Order, **Freedom of information** and General Order, **Rates—service fees**.

4(2)(a)(iv) and 4(2)(b)



4(2)(a)(iv) and 4(2)(b)



4(2)(a)(iv) and 4(2)(b)



4(2)(a)(iv) and 4(2)(b)



### **Blood/breath analysis certificates**

Certificates of analysis (CoA) are provided by INSB to investigators and prosecutors for use at criminal trials. They can be sourced through the FIDEX system, available through the intranet at 4(2)(a)(v) and 4(2)(b)


All enquiries for disclosure pertinent to other matters should be referred to Forensic Science South Australia.

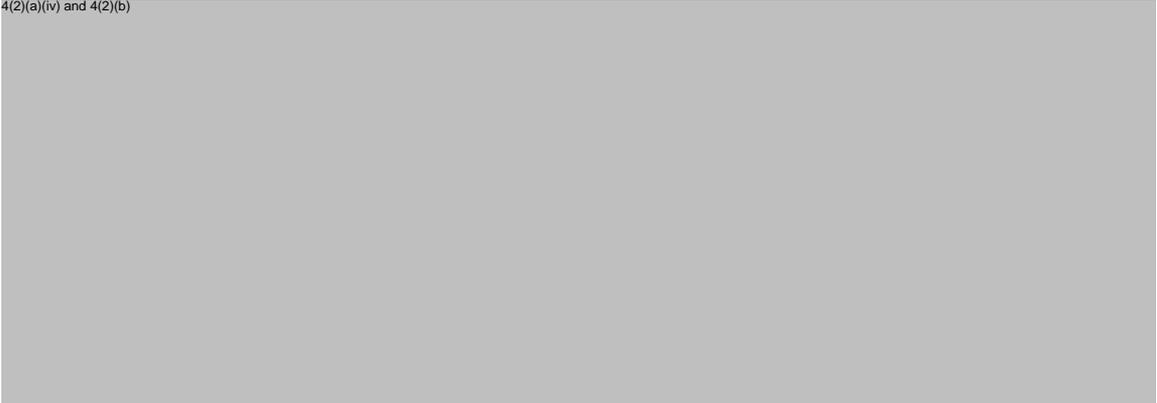
## **7. OPERATIONAL RELEASE**

Operational release may be to other SAPOL employees or to persons, agencies or organisations external to SAPOL, including the following.

### **Child abuse reporting line**

Refer to General Order, **Children and young people—protection from harm** relative to reporting of suspicion that a child or young person may be at risk.

4(2)(a)(iv) and 4(2)(b)



### **Community safety**

Where there is an actual or potential risk to community safety, the release of information to the public must be facilitated as soon as is reasonably practicable in order to reduce that risk. For information regarding media releases refer to General Order, **Media affairs**.

## Intelligence

SAPOL intelligence holdings are exempt from the requirements of the *Freedom of Information Act 1991*. These holdings may also be subject to claims of public interest immunity. An employee must not release intelligence to persons or organisations outside of SAPOL without authorisation of the Officer in Charge, SIB. This requirement includes the release of intelligence for court purposes and classified criminal intelligence in accordance with General Order, **Classified criminal intelligence**.

## Joint agency operations

In joint agency or interstate operations, the lead agency of the investigation/operation will be responsible for authorising the release of information relevant to that matter.

## Listening and surveillance devices

Information received and held pursuant to a warrant issued under the *Listening and Surveillance Devices Act 1972* must only be accessed and released in accordance with that Act. An employee can obtain advice regarding release of this information from the Officer in Charge, Telecommunications Interception Section.

4(2)(a)(iv) and 4(2)(b)



## Telecommunications interception

Information received and held under the *Telecommunications (Interception and Access) Act 1979* (Cth) must only be accessed and released in accordance with that Act. An employee can obtain advice regarding release of this information from the Officer in Charge, Telecommunications Interception Section.

## **Media**

All interaction with the media including releases must be in accordance with General Order, **Media affairs**.

## **Solicitor interviews**

Requests from solicitors to interview SAPOL employees are subject to the provisions of General Order, **Legal action by or against SAPOL employees**.

## **Victims**

A victim of a crime has the right to be kept informed of the progress of the investigation into the matter. Where a victim of crime chooses to seek further information, the employee receiving the request must comply with the *Victims of Crime Act 2001* and ensure they provide appropriate information to the victim.

Refer to General Order, **Victims**.

## **8. INFORMATION AND COMMUNICATIONS TECHNOLOGY**

Information Systems and Technology Service (IS&T) is responsible for managing access to corporate computer systems. All employees are accountable for protecting SAPOL information including documents, data, intellectual knowledge and information stored in information and communications technology (ICT) systems.

Refer to General Order 8540, **Information technology management**.

## **9. CRIME STATISTICS AND ORGANISATIONAL PERFORMANCE DATA**

Crime statistics and organisational performance data can be complex and contain sensitive information impacting on SAPOL's strategic direction and corporate policy as well as its relationship with government.

Performance data includes information such as police response times, expiation notice data and human resource material.

Appropriate statements explaining crime counting rules and identified relevant factors, for example particular crime trends and police responses, should accompany all releases and commentary on crime statistics and organisational performance data.

When the release of crime statistics or performance data will impact another government agency then the appropriate person in that agency should be contacted prior to the release.

### **Corporate level data**

Corporate level crime statistics and performance data includes information pertaining to state level policing activity, and corporately sensitive matters and policies that generally fall outside the management of individual Districts, LSAs, branches and groups.

An employee must not release corporate level crime statistics or performance data without authorisation from the Assistant Commissioner, Governance and Capability Service or the relevant assistant commissioner/director.

All enquiries by the media for crime statistics or organisational performance data should be directed to the Manager, Media and Public Engagement Section.

### **District/LSA/branch data**

District/LSA/branch level crime statistics and organisational performance data includes information solely related to a District/LSA/branch direct managerial responsibility with no wider relationship or link to any other SAPOL area, branch or operation.

An employee must not release District/LSA/branch level crime statistics or performance data without authorisation from the officer in charge of the relevant District/LSA/branch. This does not preclude information being released about crime trends in a particular area, but should not include direct statistical comparison data of streets or suburbs.

SAPOL crime statistics for each District/LSA are released publicly on a monthly basis through the SAPOL Internet site. Where a request is made for crime statistics which have already been released publicly, for example through the SAPOL annual report or monthly release of District/LSA crime statistics, the requesting person should be directed to those areas to see whether that public information satisfies their request.

### **Collating data**

Employees responsible for collating data must understand the underlying nature and context to any request, and probable use of crime statistics and performance data to be released. During collation of the information employees must ensure:

- complete accuracy and integrity of the statistics and data
- subsequent release would not compromise the identity of a victim or alleged offender, nor the integrity of a SAPOL operation or corporate policy.

For further enquiries contact the Business Information Unit.

## **10. MASKING OF SAPOL RECORDS**

An employee may apply to have access to a report/record within the Police incident management system (PIMS)/Shield restricted for an incident/occurrence.

### **Masking PIMS records**

Requests for masking of records or access to masked records can only be actioned during business hours. The Manager, Data Management Unit is responsible for approving the application and where the request is not supported, an employee may request a review of the decision by the Director, Business Service.

A PIMS record may be masked when the record meets the following criteria:

- the employee, or a near relative, is a victim or an offender and they consider that unrestricted access to the information has the potential to create undue hardship, emotional stress, embarrassment or other undue attention because of their position within SAPOL
- where the person is a dignitary, person of notoriety or has a near relationship with a person who is a dignitary or person of notoriety, and availability of that information has the potential to jeopardise their personal safety.

An application to have a record masked must be submitted on a **RF1628 Request to mask personal information (RF1628)**. The **RF1628** is available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup> and should be submitted by email to <sup>4(2)(a)(vi) and 4(2)(b)</sup> or fax 732 24180 as soon as practicable after the information has been recorded on PIMS.

### *Access to PIMS masked records*

Once masked a record cannot be electronically managed. When an employee requires a copy of the record for reference, this should be facilitated before it is masked. The record should be confidentially managed and kept secure. The Professional Conduct Section will, when appropriate, take responsibility for managing active records.

All requests for records to be unmasked, to allow access for vetting or modification, must be made to the Data Management Unit by email to <sup>4(2)(a)(vi) and 4(2)(b)</sup>. The Officer in Charge, Professional Conduct Section will audit all access to masked files.

A register of masked details is maintained by the Manager, Data Management Unit and will be reviewed annually. A report relating to an employee will normally remain masked whilst the employee remains within SAPOL. When a masking is to be reversed, the employee who applied for the masking or their successor where appropriate, will be advised and given an opportunity to request a review by the Director, Business Service.

### **Masking Shield records**

For information in relation to masking Shield records refer to General Order, **Crime and occurrence reporting** relevant to restricting occurrences and the associated risk assessment.

### *Access to Shield masked records*

When an employee requires access to an occurrence with an ACL, a HEAT request must be raised for the attention of IS&T Security Branch outlining the reasons and time period of the access.

Where an occurrence no longer meets the requirement to be masked with an ACL, the member that applied/requested the ACL can remove it when they have the appropriate permissions, or contact IS&T Security for advice.

## **11. REFERENCES**

*Children's Protection Act 1993*

*Code of Ethics for the South Australian Public Sector* available through the Internet at <<http://publicsector.sa.gov.au/policies-standards/code-of-ethics>>

*Freedom of Information Act 1991*

General Order 8540, **Information technology management**

General Order, **Children and young people—protection from harm**

General Order, **Classified criminal intelligence**

- General Order, **Crime and occurrence reporting**
- General Order, **Disclosure compliance and subpoena management**
- General Order, **Freedom of information**
- General Order, **Legal action by or against SAPOL employees**
- General Order, **Media affairs**
- General Order, **Rates—service fees**
- General Order, **Victims**

*Information Privacy Principles Instructions* available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup>

*Information Sharing Guidelines* available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup>

*Interagency Code of Practice for Investigation of Suspected Child Abuse or Neglect* available through the intranet at <sup>4(2)(a)(v) and 4(2)(b)</sup>

*Listening and Surveillance Devices Act 1972*

*Police Complaints and Discipline Regulations 2017*

*Code of Ethics for the South Australian Public Sector*

*Public Sector (Data Sharing) Act 2016*

*South Australia Police (SAPOL) ISG Appendix (procedure)* available through the intranet <sup>4(2)(a)(v) and 4(2)(b)</sup>

*Spent Convictions Act 2009*

*Teachers Registration and Standards Act 2004*

*Telecommunications (Interception and Access) Act 1979 (Cth)*

*Victims of Crime Act 2001*

## 12. FURTHER ENQUIRIES

Information Services Branch, telephone 732 23347.

## 13. DOCUMENT HISTORY SINCE 18/11/2009

Gazette reference (SAPG)	Date	Action (amendment/deletion/new/review/temporary variation)
363/09	18/11/09	Amendment—insertion of headings and text— <b>3. MASKING RECORDS</b> and <b>Access to a masked record</b>
52/10	24/02/10	Amendment—rewording of text at <b>6. DISCLOSING INFORMATION</b>
88/11	23/03/11	Review 2011.
153/13	24/07/13	General Order, <b>Releasing/accessing information</b> —reviewed, rewritten and renamed General Order, <b>Information—access and release</b> .

**OFFICIAL: Sensitive**

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

---

Gazette reference (SAPG)	Date	Action (amendment/deletion/new/review/temporary variation)
97/14	16/04/14	Amendment—General Order, <b>Teachers, government employees and government contractors</b> has been deleted and the relevant text incorporated into this General Order.
129/17	21/06/17	Review 2017.
150/18	04/07/18	Amendment—district policing model implementation.
13/20	15/01/20	Amendment—including information sharing guidelines.
133/20	29/07/20	Amendment—legislative changes—Police Complaints and Discipline Regulations 2017 update.
182/21	22/09/21	Review 2021.

**APPROVED BY COMMISSIONER/DEPUTY**

.....  
*Print Full Name*

.....  
*ID Number*

.....  
*Signature*

08/09/2021  
*Date*

**Documentation certification and verification**

General Order draft—prepared by: Mason Beck, Acting Manager, Information Release Unit  
General Order—verified by: Stephen Johninke, Director, Business Service