LC03 LEGAL REQUIREMENTS OF SECTION 86 COMMITTEES

DOCUMENT TYPE:	Section 86 Committee Governance Manual
DOCUMENT STATUS:	Approved
POLICY OWNER POSITION:	Director Corporate Services
APPROVED BY:	Management Executive Group
DATE ADOPTED:	23/06/2016
VERSION NUMBER:	2
REVIEW DATE:	23/06/2020
RELATED STRATEGIC DOCUMENTS, POLICIES OR PROCEDURES:	Section 86 Committee of Management Policy
RELATED LEGISLATION:	Local Government Act 1989
EVIDENCE OF APPROVAL:	 Signed by Chief Executive Officer
FILE LOCATION:	K:\EXECUTIV\policies and procedures\Procedures - adopted PDF and Word\Section 86 Committees of Management Governance Manual\PRC LC03 Legal requirements of section 86 Committees v2.docx

Procedure documents are amended from time to time, therefore you should not rely on a printed copy being the current version. Please consult the Loddon Shire Intranet to ensure that the version you are using is up to date.

This document is available in alternative formats (e.g. larger font) if requested.

1 PURPOSE

This section provides information to members of Section 86 committees about their legal requirements.

2 SCOPE

Section 86 committees act “for and on behalf of Council”, and are therefore acting as though they are the Council while operating within the powers and duties assigned in their Instrument of Delegation.

Therefore, Section 86 committees have the same legal requirements as the Council.

3 LEGISLATION (ACTS OF PARLIAMENT)

There are a number of key Acts of Parliament that apply to Council, and therefore, Section 86 committees of management.
The Acts listed in this information sheet relate to good governance.

Acts which apply to other topics such as safety, risk management, food handling, building, etc. will be referenced in information sheets developed on those topics.

3.1 Local Government Act 1989

The primary legislation is the Local Government Act 1989, and its requirements are covered in the Governance Manual information sheet LC01 Local Government Act 1989, which can be found at:

www.loddon.vic.gov.au/Our-documents/Council-committees-information/Governance-information

3.2 Public Records Act 1973

Council, and therefore, Section 86 committees of management have responsibilities to manage, store and protect any records created in relation to their business, and to destroy those records in accordance with legislation and records management standards.

Section 86 committees of management must not destroy any records relating to their activities, and must consult Council about appropriate destruction, which will be undertaken by Council officers.

3.2.1 Managing records

Section 86 committee records, regardless of how old they are, are public records and must be treated as such.

Each committee is required to store and maintain records it creates, until they are passed to Council for assessing and destroying at the appropriate time.

3.2.2 Electronic records

Electronic records are public records and must be treated the same as hard copy records.

3.2.3 Records disposal

Section 86 committee records cannot be destroyed by the committee. They must be forwarded to Council for assessment and destruction at the appropriate time.

3.3 Freedom of Information Act 1982

Under the Freedom of Information Act 1982, the community has the right to access documents generated or held by council. As Section 86 committees are committees of Council, this right extends to documents held by Section 86 committees.

Those community members seeking information under the Freedom of Information Act must pay a fee which is included in Council's annual fees and charges schedule which is published on Council's website.

Any application to a committee under Freedom of Information should be referred to Council's Freedom of Information Officer which is Council's Director Corporate Services.

The application will be assessed by Council, which may require the committee providing some information to Council in order to satisfy the request.

3.4 Privacy and Data Protection Act 2014

The Privacy and Data Protection Act 2014 replaced the Information Privacy Act 2000 and became fully operations on 9 December 2014.

3.4.1 Purpose of the Act

The two main purposes of the Act are to provide for:

1. responsible collection and handling of personal information in the Victorian public sector
2. remedies for interferences with the information privacy of an individual.

3.4.2 Objectives of the Act

The four main objectives of the Act are:

1. to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector
2. to balance the public interest in promoting open access to public sector information with the public interest in protecting its security
3. to promote awareness of responsible personal information handling practices in the public sector
4. to promote the responsible and transparent handling of personal information in the public sector.

3.4.3 Information Privacy Principles

Section 20(1) of the Act states that a Council must not do an act, or engage in a practice, that contravenes an Information Privacy Principle (IPP) in respect of personal information collected, held, managed, used, disclosed or transferred by it.

As a Section 86 committees are acting “for and on behalf of the Council” this Act extends to Section 86 committees.

The 10 IPP’s are:

- Principle 1—Collection
- Principle 2—Use and Disclosure
- Principle 3—Data Quality
- Principle 4—Data Security
- Principle 5—Openness
- Principle 6—Access and Correction
- Principle 7—Unique Identifiers
- Principle 8—Anonymity
- Principle 9—Transborder Data Flows
- Principle 10—Sensitive Information

Appendix 1 contains the full wording of each IPP as per the Act.

It should be noted that protection under this Act does not apply to information in the public arena, which includes information on the internet.

However, each committee's default position should be to protect any personal information that it collects for its activities, and to ensure that any disclosure would not contravene an IPP.

3.5 Protected Disclosure Act 2012

The Protected Disclosure Act 2012 replaced the Whistleblower Protection Act from 2012. The purpose of the Act is:

(a) to encourage and facilitate disclosures of—

(i) improper conduct by public officers, public bodies and other persons; and

(ii) detrimental action taken in reprisal for a person making a disclosure under this Act; and

(b) to provide protection for—

(i) persons who make those disclosures; and

(ii) persons who may suffer detrimental action in reprisal for those disclosures; and

(c) to provide for the confidentiality of the content of those disclosures and the identity of persons who make those disclosures.

Council is an entity that can receive disclosures, and is therefore, required to prepare a procedure to cover the handling of protected disclosures. Council's procedure can be found at:

www.loddon.vic.gov.au/About-us/Our-Council/Governance/Protected-disclosure

Committees should make themselves aware of Council's procedure so that they are ready if they ever receive a disclosure. Only Council's Chief Executive Officer or Director Corporate Services can deal with a disclosure.

4 DEFINITIONS OF TERMS OR ABBREVIATIONS USED

Term	Definition
Disclosure	A disclosure is a complaint, report, or allegation of improper conduct or detrimental action by a public body or officer of a public body.
Protected disclosure	As defined in the Act, a protected disclosure means a disclosure that satisfies Part 2 of the Act. Part 2 of the Act has been provided as an Appendix to this procedure. "A complaint or allegation that is already in the public domain will not normally be a protected disclosure, for example if the matter has already been subject to media or other public commentary. The term 'disclosure' is interpreted under the *Protected Disclosure Act 2012* (Vic) in the ordinary sense of the word as a 'revelation' to the person receiving it."[1]

Term	Definition
Improper conduct	As defined in the Act, improper conduct includes: • corrupt conduct • conduct that is not corrupt conduct, but if proved, would constitute a criminal offence or reasonable grounds for dismissing or dispensing with or otherwise terminating the services of the officer who was or is engaged in that conduct. It includes: a. conduct of any person that adversely affects the honest performance by a public officer or public body of his or her or its functions as a public officer or public body b. conduct of a public officer or public body that constitutes or involves the dishonest performance of his or her or its functions as a public officer or public body c. conduct of a public officer or public body that constitutes or involves knowingly or recklessly breaching public trust d. conduct of a public officer or public body that involves the misuse of information or material acquired in the course of the performance of his or her or its functions as a public officer or public body, whether or not for the benefit of the public officer or public body or any other person e. conduct that could constitute a conspiracy or an attempt to engage in any conduct referred to in paragraph (a), (b), (c) or (d) f. conduct of a public officer or public body in his or her capacity as a public officer or its capacity as a public body that— i. involves substantial mismanagement of public resources; or ii. involves substantial risk to public health or safety; or iii. involves substantial risk to the environment.
Detrimental action	As defined in the Act, detrimental action includes: • action causing injury, loss, or damage • intimidation or harassment • discrimination, disadvantage or adverse treatment in relation to a person's employment, career, profession, trade or business, including the taking of disciplinary action.

5 REVIEW

The Director Corporate Services will review this procedure for any necessary amendments no later than 4 years after adoption of this current version.

Appendix 1: Information Privacy Principles

1 Principle 1—Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of—

(a) the identity of the organisation and how to contact it; and

(b) the fact that the individual is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Principle 2—Use and Disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless—

(a) both of the following apply—

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual—

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information; or

(d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent—

(i) a serious and imminent threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety or public welfare; or

(e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or 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

(f) the use or disclosure is required or authorised by or under law; or

(g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(h) the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and—

(i) the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and

(ii) an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

2.2 If an organisation uses or discloses personal information under IPP 2.1(g), it must make a written note of the use or disclosure.

3 Principle 3—Data Quality

3.1 An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

4 Principle 4—Data Security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

5 Principle 5—Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Principle 6—Access and Correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that—

(a) providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders—

by or on behalf of a law enforcement agency; or

(j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of IPP 6.1(a) to (j) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, the organisation—

(a) must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee; and

(b) may refuse access to the personal information until the fee is paid.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

6.8 If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must—

(a) provide access, or reasons for the denial of access; or

(b) correct the personal information, or provide reasons for the refusal to correct the personal information; or

(c) provide reasons for the delay in responding to the request for access to or for the correction of personal information—

as soon as practicable, but no later than 45 days after receiving the request.

7 Principle 7—Unique Identifiers

7.1 An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.

7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless—

(a) it is necessary to enable the organisation to carry out any of its functions efficiently; or

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless—

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or

(b) one or more of IPP 2.1(d) to (g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

8 Principle 8—Anonymity

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation.

9 Principle 9—Transborder Data Flows

9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if—

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of precontractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply—

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

10 Principle 10—Sensitive Information

10.1 An organisation must not collect sensitive information about an individual unless—

(a) the individual has consented; or

(b) the collection is required under law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns—

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if—

(a) the collection—

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.