OUTER URBAN PROJECTS

4 GAFFNEY STREET
COBURG NORTH 3058

INFO@OUTERURBANPROJECTS.ORG

OUTERURBANPROJECTS.ORG

PRIVACY POLICY

PRINCIPLE

Everyone has the right to have their personal information kept private.

PURPOSE

The purpose of this document is to provide a framework for Outer Urban Projects (OUP) in dealing with privacy considerations. This framework is consistent with the Victorian *Privacy and Data Protection Act 2014*.

If OUP is delivering programs in states and territories other than Victoria, OUP must adhere to the local laws of the jurisdiction in which the program(s) operate.

POLICY

OUP recognises the essential right of individuals to have their information administered in ways which they would reasonably expect – protected on one hand and made accessible to them on the other.

OUP is committed to protecting the privacy of personal information which the organisation collects, holds and administers in the course of delivering its programs and activities.

INFORMATION PRIVACY PRINCIPLES

The Victorian Information Privacy Principles are the core of privacy law in Victoria and set out the minimum standards for managing personal information under the law.

Victorian Information Privacy Principles

1. Collection
2. Use and disclosure
3. Data quality
4. Data security
5. Openness
6. Access and correction
7. Unique identifiers

8. Anonymity
9. Transborder data flows
10. Sensitive information

RESPONSIBILITIES

All OUP personnel are responsible for complying with all OUP privacy requirements.

The OUP Board of Directors is responsible for developing, adopting and reviewing this policy.

The CEO(s) is responsible for the implementation of this policy and the related procedures, for monitoring changes to privacy legislation, and for advising on the need to review or revise this document as needed.

DEFINITIONS

Personal information means that which directly or indirectly identifies a person.

Sensitive information means information or an opinion about an individual's:

- Racial or ethnic origin; or
- Political opinions; or
- Membership of a political association; or
- Religious beliefs or affiliations; or
- Philosophical beliefs; or
- Membership of a professional or trade association; or
- Membership of a trade union; or
- Sexual preferences or practices; or
- Criminal record: or
- Medical information—

that is also personal information.

PROCEDURES

1. Collection – OUP will:
    - Only collect information that is necessary for one or more of its functions or activities
    - Collect personal information only by lawful and fair means and not in an unreasonably intrusive way
    - When collecting someone's personal information from them, make sure the person is aware of:
        i. The identity of the organisation and how to contact OUP
        ii. The fact that the person can gain access to their information held by OUP
        iii. The purpose for which the information is collected
        iv. To whom (if any) the organisation might be required to disclose the information
        v. Any law that requires particular information to be collected
        vi. The consequences (if any) for the person if any required personal information is not provided
    - Collect personal information from the person themselves wherever possible
    - If collecting personal information from a third party, take reasonable steps to advise the person whom the information concerns, from whom their personal information has been collected

(unless making the person aware would pose a serious threat to someone's life or health)

2. Use and disclosure – OUP will:
    - Only use or disclose information for the primary purpose for which it was collected, or a directly related secondary purpose where the individual would reasonably expect the information to be used or disclosed
    - For other uses, OUP must obtain consent from the affected person, unless:
        i. OUP reasonably believes there is a serious threat to life, health, safety, or wellbeing
        ii. OUP has reason to suspect unlawful activity has been/is being/is going to be engaged in, and is reporting its concerns to the relevant authority for prevention/detection/enforcement or other official purposes

    For the purpose of this clause, OUP must make a written note of the use or disclosure.

3. Data quality – OUP will take reasonable steps to ensure the personal information it collects, uses, or discloses is accurate, complete, up to date, and relevant to the functions it performs.

4. Data security – OUP will:
    - Take reasonable steps to protect the personal information it holds from misuse, loss, and unauthorised access, modification or disclosure
    - Take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.
    - Only destroy records in accordance with the OUP Documents/Records Management and Control Policy and Procedure

5. Openness – OUP will:
    - Ensure stakeholders are aware of OUP's Privacy Policy and its purposes
    - Make this information freely available to anyone who asks for it
    - On request, take reasonable steps to let people know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information

6. Access and correction – OUP will:
    - Ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date
    - If the individual and OUP disagree about whether the information is accurate, complete and up to date, and the individual asks OUP to associate with the information a statement claiming that the information is not accurate, complete or up to date, OUP will take reasonable steps to do so
    - OUP will provide to the individual its reasons for denial of access or a refusal to correct personal information
    - OUP can withhold the access of an individual to his/her information if:
        i. providing access would pose a serious and imminent threat to the life or health of any individual; or
        ii. providing access would have an unreasonable impact upon the privacy of other individuals; or
        iii. the request for access is frivolous or vexatious; or
        iv. the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the

process of discovery in those proceedings; or

v. 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
vi. providing access would be unlawful; or
denying the access is required or authorised by law; or
vii. providing access would be likely to prejudice:
    a) an investigation of possible unlawful activity
    b) the prevention/detection/investigation/prosecution/punishment of criminal offences or breaches of a law
    c) the enforcement of laws relating to the confiscation of proceeds of crime
    d) the protection of public revenue
    e) the prevention/detection/investigation/remedying of seriously improper conduct
    f) the preparation for/conduct of proceedings before any court or tribunal, or implementation of its orders

    by or on behalf of a law enforcement agency; or
viii. an enforcement body performing a lawful security function asks OUP not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia

- Where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, OUP may give the individual an explanation for the commercially sensitive decision rather than direct access to the information
- If OUP decides not to provide the individual with access to the information on the basis of the above-mentioned reasons, OUP will consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties
- OUP may charge for providing access to personal information, however
    i. The charges will be nominal and will not apply to lodging a request for access
    ii. OUP must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee
    iii. OUP may refuse access to the personal information until the fee is paid.
- If OUP holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, OUP must take reasonable steps to correct the information so that it is accurate, complete and up to date
- 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
- An organisation must provide reasons for denial of access or a refusal to correct personal information
- If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must:
    i. provide access, or reasons for the denial of access; or
    ii. correct the personal information, or provide reasons for the refusal to correct the personal information; or
    iii. 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. Unique identifiers – OUP will 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
    - Adopt as its own identifier of an individual, an identifier that has been assigned by any third party, unless:
        i. It is necessary to enable OUP to carry out any of its functions efficiently; or
        ii. OUP has obtained the consent of the individual to the use of the unique identifier; or
        iii. OUP is outsourcing services and adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under the requirements of a contract.
    - Use or disclose the identifier assigned to an individual by a third party unless:
        i. the use or disclosure is necessary for OUP to fulfil its obligations to the third party; or
        ii. OUP has obtained the consent of the individual to the use or disclosure; or
        iii. Provisions under Principle 2 – Use and Disclosure apply.

8. Anonymity – OUP will allow people from whom the personal information is being collected to not identify themselves or use a pseudonym unless it is impracticable to deal with them on this basis.

9. Transborder data flows – OUP may:
    - Transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if:
        i. OUP 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
        ii. The individual consents to the transfer; or
        iii. 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
        iv. 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
        v. All of the following apply:
            a) the transfer is for the benefit of the individual
            b) is impracticable to obtain the consent of the individual to that transfer
            c) if it were practicable to obtain that consent, the individual would be likely to give it or
        vi. OUP 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. Sensitive information – OUP:
    - Must not collect sensitive information about an individual unless—
        i. The individual has consented; or
        ii. The collection is required or authorised under law; or
        iii. The collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns—
            a) is physically or legally incapable of giving consent to the collection; or

b) physically cannot communicate consent to the collection; or

iv. The collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

- May collect sensitive information about an individual if:
  i. The collection:
     a) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
     b) 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
  ii. There is no reasonably practicable alternative to collecting the information for that purpose; and
  iii. It is impracticable for OUP to seek the individual's consent to the collection.

RELATED DOCUMENTS

Privacy and Data Protection Act 2014 (Vic)

Victorian Information Privacy Principles

OUP Documents/Records Management and Control Policy and Procedure