

13. PRIVACY AND CONFIDENTIALITY

PURPOSE

EDVOS adopts the principles of Privacy Act 1998 (Cth), the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic) and is committed to protecting the privacy and confidentiality of its clients, staff, volunteers, students, Board members and other stakeholders while information is collected, used and stored.

SCOPE

This policy applies to all people who are clients of EDVOS and to all staff (paid and unpaid), contractors, participants and online users. The policy has been developed to provide guidance on EDVOS's legal and ethical expectations in dealing with confidentiality and privacy matters.

EXCLUSIONS

Some variations apply in line with Part 5A of the Family Violence Protection Act 2008 (the Family Violence Information Sharing Scheme) and the Family Violence Protection (Information Sharing and Risk Management) Regulations 2018. Please refer to the EDVOS Family Violence Information Sharing Scheme Procedures for further information.

DEFINITIONS

Breach or Possible Breach means an action or omission that results in loss, theft, misuse or unauthorised disclosure of personal information or sensitive information, or has the potential to do so.

Common examples of breaches or a possible breach includes:

- a) Leaving paper records in a public place;
- b) Deleting personal data when it is still needed;
- c) Losing a memory stick containing personal data;
- d) Loss or theft of mobile devices containing data about people (e.g., laptops or mobile phones) or loss of hard copy data within briefcases, folders;
- e) Sharing information about people with unauthorised third parties, either accidentally or wilfully;
- f) Sending emails or letters in error to the wrong person(s) or wrong address(es); and
- g) Any 'near miss' incident that had the potential to cause a data breach even though it might not have done so.

Client/s refers to a person/s who accesses/accessed EDVOS services.

Complaint is a statement that something is unsatisfactory or unacceptable. Must have had an impact on an individual or group.

Confidentiality implies the relationship of confidence between the organisation and individuals.

Consent implies voluntary agreement to an act, practice or purpose.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	1 of 10

13. PRIVACY AND CONFIDENTIALITY

Health Information:

1. information or an opinion about—
 - a. the physical, mental or psychological health (at any time) of an individual; or
 - b. a disability (at any time) of an individual; or
 - c. an individual's expressed wishes about the future provision of health services to him or her; or
 - d. a health service provided, or to be provided, to an individual— that is also personal information; or
2. other personal information collected to provide, or in providing, a health service; or
3. other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
4. other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants—

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

Near Miss means a situation where a breach would have occurred without intervention. This includes situations where a privacy incident has occurred without any disclosure of personal information or sensitive information.

Personal Information refers to information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not (Privacy Act 1988).

Privacy regarded as the freedom from interference or intrusion (Commissioner for Privacy and Data Protection)

Privacy Officer This role ensures that the organisation upholds its privacy obligations and complies with the Privacy Act 1998 (Cth), Privacy and Data Protection Act 2014 (Vic), Australian Privacy Principals (APPs) and the Information Privacy Principals (IPPs). They are the first point of contact within the organisation for all matters related to privacy and personal information, complaints from employees within the organisation, and members of the public.

Sensitive Information refers to information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health, genetic or biometric templates, that is also personal information (Privacy Act 1988).

Staff for the purpose of this procedure the term 'staff' or 'all staff' refers to all persons working within EDVOS including paid, unpaid, students, volunteers and contractors.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	2 of 10

13. PRIVACY AND CONFIDENTIALITY

BACKGROUND INFORMATION

EDVOS is committed to ensuring privacy and confidentiality for all people involved with EDVOS in any way. There is a range of procedures that align with this policy that support best practice in privacy at EDVOS, as well as a nominated Privacy Officer, Deputy Privacy Officer and Privacy Response Team.

EDVOS follows the Department of Health and Human Services CIMS Guide 2016 for the identification and categorisation of client incidents, and reports all privacy incidents to DHHS as required.

EDVOS supports a culture of reporting and learning in regard to privacy

POLICY STATEMENT

EDVOS will comply with the Privacy Act 1988, Australian Privacy Principles, Privacy and Data Protection Act 2014 (Vic), the Health Privacy Principles in the Health Records Act 2001 (Vic), Family Violence Information Sharing Scheme, Child Information Sharing Scheme and Notifiable Data Breach Scheme which set clear standards for the collection, access, storage and use of personal information which is obtained as part of normal operations.

The following Public Privacy Statement outlines how EDVOS complies with the legislative requirements. The Statement is used in various formats including but not limited to EDVOS website and privacy brochure.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	3 of 10

13. PRIVACY AND CONFIDENTIALITY

WHAT KINDS OF PERSONAL INFORMATION DO WE COLLECT?

The type of information that we collect and hold will depend on the nature of your involvement with us.

Depending on the reason for collecting the personal information, the personal information that we collect may include (but is not limited to) name, age, residential address, date of birth, phone number, email address, bank account details, emergency contact details, Health information, reason for contacting EDVOS, income information, cultural information, language spoken and images. Our advocates will also collect information from clients describing their situation and their contact with you.

We may also collect sensitive information (including Health information) from a person including a working with children check, health information, family violence risk assessment, financial information, counselling information, prison records, government identifiers or a police check.

If you choose not to provide information when requested, we may not be able to service your needs. For example, if you want to remain anonymous or use a pseudonym.

We sometimes receive unsolicited personal information. When we do receive unsolicited personal information, we will usually securely destroy or de-identify the information if it is reasonable and lawful to do so, unless the unsolicited information is reasonably necessary for our functions or activities.

Health information will be securely destroyed or deleted in accordance with Health Privacy Principle 4. Consistent with the Surveillance Devices Act 1999 (Vic), EDVOS will not install surveillance devices in toilet, washroom and change room except:

- in accordance with a warrant or emergency authorisation;
- in accordance with a law of the Commonwealth; or
- if required by a condition on a license granted under the Liquor Control Reform Act 1988 (Vic).

HOW DO WE COLLECT PERSONAL INFORMATION?

Personal information is collected:

- By our teams and advocates when a person walks in to one of our offices with an enquiry;
- Via our assessment intake form;
- Via our website;
- By email, post and phone; and
- Through referrals.

We will attempt wherever practicable to collect personal information directly from you. Information is collected in a number of ways including from when you fill in a form, make an enquiry online, attend a face-to-face meeting, provide email correspondence, phone us, or make a payment.

We may collect personal information from individuals such as visitors, contractors, and suppliers.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	4 of 10

13. PRIVACY AND CONFIDENTIALITY

We will endeavour to only ask for your personal information if it is reasonably necessary for the activities that you are looking to be involved in. We may also collect information, or be required to collect information in accordance with the Family Violence Information Sharing Scheme and/or Child Information Sharing Scheme.

FOR WHAT PURPOSE DO WE COLLECT PERSONAL INFORMATION?

Personal information will be collected only for the purpose of which are directly related to the functions or activities of EDVOS and securely destroyed or de-identified when it is no longer needed for the purpose that it was collected and all statutory obligations have been met.

We may collect, hold, use or disclose your personal information for the following general purposes:

1. To identify you;
2. For the purpose for which the personal information was originally collected;
3. For a purpose for which you have consented;
4. For information for direct marketing, and you will be given an opt-out in such communications;
5. For any other purpose authorised or required by an Australian law (some of which are detailed below); and
6. For any other purpose authorised or required by a court or tribunal.

HOW WILL WE USE AND DISCLOSE YOUR PERSONAL INFORMATION?

We will use and disclose your personal information for the purpose for which it was collected or a secondary purpose as permitted. Client files are stored in a secure environment and only authorised staff have access to files.

We may also share information, or be required to share information in accordance with the Family Violence Information Sharing Scheme and/or Child Information Sharing Scheme.

EDVOS upholds the right of individuals to have their privacy and confidentiality recognised and maintained. Relevant policy and or legislation will be followed in circumstances where the right to privacy may be overridden by other considerations. These may include:

- Consent has been provided by client, carer or an authorised person;
- A related secondary purpose the individual would reasonably expect;
- Where it is necessary for individual or public safety;
- In compliance with a court order, subpoena, summons or as required by law;
- For risk assessment or management purposes;
- In compliance with the Notifiable Data Breach Scheme; or
- It is required by law including but not limited to Family Violence Information Sharing Scheme and the Child Information Sharing Scheme.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	5 of 10

13. PRIVACY AND CONFIDENTIALITY

EDVOS is classified as an Information Sharing Entity and a Risk Assessment Entity under the Family Violence Information Sharing Scheme and Child Information Sharing Scheme (together, **the Schemes**). Information may be collected, held, used or disclosed in accordance with our obligations under the Schemes. This may include using or disclosing your personal information for a secondary purpose, when EDVOS reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual.

Personal information will be securely destroyed or de-identified when it is no longer needed for the purpose that it was collected and all statutory obligations have been met.

DEPARTMENT OF HEALTH AND HUMAN SERVICES – REPORTING REQUIREMENTS

EDVOS receives funding from the Department of Health and Human Services (**DHHS**). As part of that funding agreement, EDVOS is required to share personal information and sensitive information, including notifying the DHHS if there is a 'privacy incident'.

Reporting to DHHS allows EDVOS to:

- Ensure timely and effective management of privacy incidents
- Address the concerns and develop actions to prevent future privacy breaches
- Assist in identifying systematic issues and improve how client information is handled; and
- Comply with its obligations under the funding agreement.

A 'privacy incident' may be a Breach, a Possible Breach or a 'Near Miss'. Breaches/Possible Breaches refer to breaches of this Policy and/or the funding agreement that EDVOS has with DHHS. EDVOS must also notify the DHHS if there are any allegations of privacy breaches that need to be investigated.

When sharing personal and/or sensitive information with the DHHS, EDVOS is required to complete a Privacy Incident Report Form which will detail:

- the privacy incident;
- the clients impacted;
- the immediate risks;
- how the incident is being managed and if a breach has occurred, how it is being contained; and
- information relating to security and breaches.

EDVOS will make this Report within one business day of becoming aware of, or being notified of a possible privacy incident, or within one business day of an allegation being made of a potential breach.

Possible privacy breaches will be reported, as well as confirmed breaches.

The Privacy Incident Report Form can be accessed at <https://providers.dhhs.vic.gov.au/reporting-incidents>.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	6 of 10

13. PRIVACY AND CONFIDENTIALITY

HOW CAN YOU ACCESS AND CORRECT YOUR INFORMATION?

Individuals have the right to seek access to their personal information and to request that it be corrected if it is incorrect. The exceptions to this include if:

- It would pose a serious threat to the life or health of any individual;
- It would have an unreasonable impact on the privacy of other individuals;
- The request is frivolous or vexatious; or
- It would be unlawful.

Upon request, individuals will be entitled to view and / or to obtain a copy of any information held by EDVOS about them. A request can be made to our Privacy Officer at privacy@edvos.org.au.

DATA QUALITY AND SECURITY

EDVOS will take reasonable measures to ensure that the personal information collected is accurate, complete and up-to-date.

Personal information held by EDVOS will be protected against loss, unauthorised access, use, or disclosure by means of reasonable technical, physical and administrative safeguards including:

- Using passwords to prevent unauthorised access and use of computers and relevant software;
- Establishing access levels to restrict access so that only relevant staff have access to certain information;
- Ensuring information is transferred securely;
- Installing virus protections and firewalls;
- Locking filing cabinets and other areas in which personal information is stored;
- Ensuring documentation containing personal or confidential information is securely destroyed;
- Not storing personal information in public areas; and
- Positioning computer terminals and fax machines so that they cannot be seen or accessed by unauthorised people or members of the public

BREACH OF PRIVACY AND CONFIDENTIALITY

If you have any questions relating to this policy, or you would like to lodge a complaint you need to contact us at privacy@edvos.org.au.

In the event of a breach of this policy or a complaint the matter will be reported to the line manager and / or Privacy Officer and an investigation conducted in accordance with EDVOS' Incident Management Policy and Procedure and Data Breach Response Plan.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	7 of 10

13. PRIVACY AND CONFIDENTIALITY

EDVOS will also assess the concern against DHHS requirements and may be required to complete a Privacy Incident Report Form.

If you are not satisfied with the response you can refer the complaint to the Office of the Australian Information Commissioner. The Victorian Office of the Health Services Commissioner website is <http://www.health.vic.gov.au/hsc/>

RESPONSIBILITIES

Board & Chief Executive Officer	<ul style="list-style-type: none"> Establish a sound system for privacy related riskoversight. Management and internal control.
Privacy Officer	<ul style="list-style-type: none"> Managing and responding to privacy complaints. Handling privacy enquiries. Ensuring all confidential information is appropriately collected, stored accessed and used. Coordinating staff privacy training
Managers & Team Leaders	<ul style="list-style-type: none"> Ensure the quality of personal information that are collected, stored and used. Assist with investigations related to privacy complaints.
All board members staff, students, volunteers and contractors	<ul style="list-style-type: none"> Abide by this policy and all associated legislation at all times. Report any breaches of privacy and confidentiality policy/legislation.

RELATED DOCUMENTS AND RESOURCES

INTERNAL

02.01 Outlook Emails & Calendar Settings Procedure

02.02 Client Data Collection & Reporting Procedure

02.03 Information Technology (IT) Security Procedure

04.09 Personnel Records Procedure

04.12 Grievance Resolution Procedure

06.02 Incident Reporting & Management Procedure

07.01 Legislative Compliance Procedure (TBD)

08.01 Code of Conduct

13.01 Responding to Subpoenas Procedure

13.02 Access to Client File Records Procedure

13.03 Sharing and Receiving Information Pursuant to the Child Information Sharing Scheme (CISS) Procedure

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	8 of 10

13. PRIVACY AND CONFIDENTIALITY

13.04 Sharing and Receiving Information Pursuant to the Family Violence Information Sharing Scheme (FVISS) Procedure

13.05 Data Breach Response Planning Procedure

15.00 Consumer Experience Policy

15.01 Feedback – Compliments, Complaints & Suggestions Procedure

Access to Client File Records Request Form

Access to Client File Records Collection & Delivery Confirmation Form

CISS Information Sharing Request (External) Form

Client Consent for Sharing Information Form

Confidentiality – Third Party

Consent for Collecting, Storing and Sharing Client Information Procedure (TBD)

Consent for Collecting, Storing and Sharing Client Information Form (Various) (TBD)

Consent for Sharing Sensitive Client Information Form (TBD)

Employee Information Management Procedure (TBD)

Freedom of Information (FOI) Procedure (TBD)

FSP Client Consent for Sharing Information with EDVOS Form

How EDVOS Protects My Privacy – Brochure

Masterfile Maintenance P&P (to be reviewed)

Notifiable Data Breach Guidelines and Form (TBD)

Counselling - Client Consent Template

Photograph, Video & Audio Consent Form

Photograph, Video & Audio Group Consent Form

PSI Client Consent for Sharing Information Form (Personal Safety Initiative)

Secure and Send Email Attachment Work instruction

Suspected Data Breach Report Form

Your Rights and Responsibilities Template

EXTERNAL

[Child Information Sharing Scheme \(CISS\) 2018](#)

[DHHS Client Incident Management System \(CIMS\) Guide](#)

[Family Violence Information Sharing \(FVIS\) Guidelines](#)

[OAIC Australian Privacy Principles \(of the Privacy Act 1988\) \(Cth\)](#)

[OAIC Notifiable Data Breach Scheme](#)

[OVIC Information Privacy Principals \(IPP\) \(Schedule 1 of the *Privacy and Data Protection Act 2014*\)](#)

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	9 of 10

13. PRIVACY AND CONFIDENTIALITY

LEGISLATION

ACTS

[Health Records Act 2001](#) (Vic)

[Family Violence Protection Act 2008](#) (Vic) - Part 5A: Family Violence Information Sharing Scheme

[Privacy Act 1988](#) (Cth)

[Privacy and Data Protection Act 2014](#) (Vic)

REGULATIONS

[Family Violence Protection \(Information Sharing and Risk Management\) Regulations 2018](#) (Vic)

STANDARDS

[Department of Health and Human Services \(DHHS\) Service Standards](#)

[QIC Health and Community Service Standards, 7th edition](#)

[Rainbow Tick Guide to LGBTI - Inclusive Practice 2nd Ed. 2016](#) (GLHV)

[Victorian Protective Data Security Standards \(VPDSS\)](#)

AUTHORISATION*

Board Chair

DATE

24/02/2021

*It is noted that items listed under 'Related Documents and Resources' and 'Legislation' may be amended without the policy needing to be reauthorised by the Board.

Document No:	POL-PC-01	Version No:	4
First approved:	14/05/2016	Next review date:	24/02/2024
Last approved:	24/02/2021	Responsible person:	Chairperson
Authorised By	Board of Governance	Page	10 of 10