Disability Rights Advocacy Service

POLICY NAME	**PRIVACY & CONFIDENTIALITY**	
NSDS STANDARD	Standard 1 - Rights	**POLICY # A105**
POLICY CLUSTER	Service Provision	

POLICY STATEMENT	Disability Rights Advocacy Service's (DRAS) mission is to safeguard and promote the rights and interests of people with disability, their family and carers. DRAS does this through its Individual Advocacy, Systemic Advocacy and NDIS Appeals Programs. DRAS will meet its obligations to comply with the Australian Privacy Principles (APP) and any registered APP code (if any) that binds our organisation. To this end, DRAS will establish and maintain open and transparent systems and practices concerning the collection, use and disclosure, quality, accuracy and correction of personal information in all areas of its operations. DRAS will maintain systems for dealing with inquiries or complaints about our compliance with the AAP. Our clients will receive assistance from DRAS in a manner that demonstrates respects for their privacy and confidentiality. This policy applies to all areas of DRAS which collect, use, disclose, store and/or provide access to personal information, including sensitive information and health information about an individual.
SCOPE	The policy applies to the DRAS Board, the Chief Executive Officer (CEO) and employees (paid or volunteers), contractors.

RELEVANT LEGISLATION	• Cth. Privacy Act (1998) and Cth. Privacy Amendment (Enhancing Privacy Protection) Act (2012) • Cth. Disability Services Act (1986) and related National Standards for Disability Services • S.A. Children's Protection Act (1993) • National Principles for Child Safe Organisations
RELATED DRAS POLICIES	• Code of Conduct (Policy# GM001) • Complaints Handling (Policy# A402) • Protection of Human Rights & Freedom From Abuse (Policy# A101)

INDICATOR(S) OF PRACTICE	1.9 DRAS keeps personal information confidential and private.
EVIDENCED BY	Restricted access to offices, locked filing cabinets, restricted access to computer data and an annual change in the passwords used to access the client database Clients signed Information Access/ Release Consent Forms. Employees and volunteers have signed DRAS' Code of Conduct acknowledging the requirement to maintain client and agency confidentiality.

CEO ENDORSEMENT	**This policy is effective as of 25/08/2020**
NEXT REVIEW DATE	**June 2023**

POLICY NAME	PRIVACY & CONFIDENTIALITY
	POLICY # A105
ASSOCIATED PROCEDURES [inc. Delegation, Functions and Requirements]	

1. INTRODUCTION

Disability Rights Advocacy Service (DRAS) Inc. acknowledges that its current and former clients and employees have legislated rights to privacy and confidentiality. It is essential that DRAS protects these rights and acts correctly in those circumstances where these rights may be overridden by other considerations.

DRAS is committed to protecting and upholding the rights of its clients to privacy and confidentiality in the way we collect, store and use information about them and the services we provide to them.

2. DEFINITIONS

Access is defined here as an APP entity allowing an individual access to records containing Personal Information held about them by the APP entity. This may include inspecting personal information held or providing a copy of the information.

Australian Privacy Principals refers to the principles contained in the Privacy Act 1988.

Client is defined here as individual client or family, legal guardian or person with enduring power of attorney in relation to a client.

Collection An APP entity (here to referred to as an agency) collects personal information if it gathers, acquires or obtains personal information from any source and by any means. This includes information not requested or obtained in error. DRAS is an APP entity.

Disclosure occurs when an agency releases information to third parties.

Employee Record is a record of personal information relating to the employment of the employee and can include documents about an employee's:

- engagement, training, disciplining or resignation,
- termination of employment,
- terms and conditions of employment,
- personal and emergency contact details,
- performance or conduct,
- hours of employment,

- salary and wages,
- membership of a professional or trade association,
- trade union membership,
- recreation, long service leave, sick, personal, maternity, paternity or other leave, or
- taxation, banking or superannuation affairs.

Health Information refers to:
(a) Information or opinion about:
(i) the health or a disability (at any time) of an individual; or
(ii) an individual's expressed wishes about the future provision of health services to him or her; or
(iii) a health service provided, or to be provided, to an individual; that is also personal information; or
(b) Other personal information collected to provide, or in providing, a health service; or
(c) 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.

Person Responsible is a person who is responsible for an individual if the person is:

- a parent of the individual; or
- a child or sibling of the individual and at least 18 years old; or
- a spouse or de facto spouse of the individual; or
- a relative of the individual, at least 18 years old and a member of the
- individual's household; or
- a guardian of the individual; or
- exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
- a person who has an intimate personal relationship with the individual; or
- a person nominated by the individual to be contacted in case of emergency.

Personal Information is defined here as any details about a person's life and includes health/ disability status, biographical data and contact details.

Primary Purpose is the main or dominant reason for which the APP entity collects Personal Information

Secondary Purpose is any reason for which information is collected or used that is not the Primary Purpose for its collection and/or use referred to above.

Sensitive Information means:
(a) 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;
- membership of a professional or trade association; or
- membership of a trade union; or
- sexual preferences or practices; or
- criminal record; or

(b) Health information about an individual.

3. ACCESS TO POLICY

DRAS will make clients and its employees aware of the policy by:

- Providing a summary of this policy in the 'Client Induction Booklet'
- Explaining the policy in a manner or form appropriate to the client,
- Displaying a sign highlighting the Australian Privacy Principles at each of DRAS' worksites, where appropriate.
- For employees and volunteers, at their induction and periodically thereafter.
- For employees, access to this policy is available on the 'L' Drive.

If a person requests a copy of this policy in a particular form, DRAS will take such steps, as are reasonable in the circumstance, to provide the policy in that form.

4. GENERAL GUIDELINES

DRAS will:

- Regard any information obtained about a person, both past and presently associated with DRAS, as confidential and will not use such information for any purpose other than that for which it was/ is given.
- Collect personal Information lawfully, fairly and openly, and where possible, directly from and with consent of the individual concerned.
- Only collect information about a person that is reasonably necessary to fulfil a DRAS function or activity.
- To the extent practical, ensure that personal information collected, used and/or disclosed is accurate, complete and up to date.
- Seek the consent of the person prior to obtaining and/or releasing information from any other source, including to persons or agencies overseas.
- Where a client wishes a cross-border release of their personal information DRAS will inform them that DRAS can not ensure that the overseas recipient would uphold the Australian Privacy Principles.
- Not use personal information or disclose the information to another party for the purpose of direct marketing.

- Ensure no unauthorised use or disclosure of personal information and that such information is stored securely and is not accessible to unauthorised persons or the general public.
- Ensure that only DRAS staff who need access to the above information will be granted access.
- Inform clients and staff of the nature of the personal information that is held by DRAS about them, including any secondary purpose for the use of that information.
- Advise clients and staff of their right to view, at any time, the information that DRAS keeps in respect to them.
- Ensure that personal information is held in accordance with DRAS' policies, contractual and good governance requirements or as deemed necessary for legal reasons.
- Inform people of how to contact DRAS with their concerns on privacy matters, including how to access personal information held about them.
- Promptly investigate, remedy and document any grievance regarding privacy or confidentiality.
- Use a variety of physical and electronic measures to restrict access, misuse, modification, loss or to minimise unauthorised access to their personal information.
- Provide information to clients regarding privacy and confidentiality processes, including how to make a compliant internally and/ or to refer the Complainant to the Office of the Australian Information Commissioner,
- Ensure any personal information collected as part of a systemic advocacy effort will be treated and managed in line with this policy and congruent with the Australian Privacy Principles.
- Ensure all members of the Board, the CEO, employees and specified contractors sign DRAS' Code of Conduct.

5. DELEGATION & FUNCTION

The DRAS Board delegates to the CEO as DRAS' Privacy Officer.

The Privacy Officer is required to manage the collection, access, alteration, storage, use, disclosure and destruction of clients' personal information.

All staff are responsible for their role in ensuring Australian Privacy Principles (and this policy) are complied with.

The CEO will ensure that DRAS Board members, employee and contractors, where relevant, are informed of the Australian Privacy Principles and sign DRAS' Code of Conduct, which reinforces our organisation's commitment to maintaining client, employee and organisational privacy and confidentiality.

New employees will be provided with a copy of DRAS' Code of Conduct to sign as part of their induction. The signing of a Code of Conduct will be recorded on the employee's 'Induction Checklist' form (Form# HR005:1) and subsequently stored in the employee's Personnel file.

Code of Conduct forms that are signed by Board Members will be kept in a folder established for this purpose by the CEO.

Employees will provide each client with a Client Induction Booklet and explanation of this policy as soon as practicable at the beginning of the case.

The CEO will ensure an electronic copy of the Privacy Act (1988) and the Privacy Amendment Act (2012) is available at to all DRAS employees. In addition, the CEO will ensure a poster of the Australian Privacy Principles (Poster# A401:2) is displayed at each DRAS office, where relevant.

6. ANONYMITY, PSEUDONYMITY AND NON-DISCLOSURE

Where practical, clients will have the option of not identifying themselves, or using a pseudonym when dealing with DRAS or when represented by DRAS against another party. Persons who wish to remain anonymous when pursuing an internal or external complaint are to be informed of the consequences (if any) of their preference for anonymity.

Where the client has given instructions that he/she is not to be contacted at a particular place, or that certain details (e.g. address) are not to be disclosed on forms or other documents, those instructions must be complied with, provided there is not conflict with a professional duty or any legislative requirement. Where such a conflict arises, this shall be explained to the client, except where this may endanger any person.

If a DRAS employee is telephoning a client and cannot speak to them directly, they should not identify themselves as calling from DRAS. The client may be seeking advice regarding family violence whilst residing with the perpetrator or experiencing bullying in the workplace. Instead, the employee should only give their first name.

Employees are to be mindful that:

- Clients can often be identified from the details of their cases, even though their names are not mentioned.
- It is not a breach of confidentiality for a matter to be discussed in the normal course of DRAS work with DRAS' CEO and other relevant DRAS employees.

7. SERIOUS COMMUNICABLE CONDITIONS

Where the client has a serious communicable condition, the individual's right to privacy must be maintained except in circumstances and where there is a definite serious risk that could threaten the health of DRAS' employees.

In these instances the following procedure must be observed:

- Where possible, written permission must be obtained from the client; and
- Wherever possible, reliance should be placed on the use of universal precautions rather than the release of information.

8. PHYSICAL MEETINGS & PREMISES

Meetings with clients, whether held at DRAS' premises or at other venues, will be held in a manner that maintains confidentiality.

When conducting physical meetings, specifically with children and young people, DRAS employees must maintain confidentiality but are also responsible for implementing child safety practices. This can include, with the child's or young person's consent, having another adult present during the meeting and / or having the meeting room door partly open.

Where a client is attending a meeting with an employee in one of DRAS' offices and another client telephones at the same time as the meeting is being conducted, then the employee will politely make arrangements with the client to return their call as soon as the meeting has concluded.

Where DRAS employees are collocated with the employees of another agency, then DRAS will seek a memorandum of understanding with the other agency for the joint adherence of confidentiality with respect to each agency's clientele.

9. COLLECTION/ RELEASE AND USE OF INFORMATION

When collecting personal information or as soon as practicable afterwards, reasonable steps will be taken by the employee to ensure that the client is aware:

- That any information obtained by DRAS about past and present clients is regarded as confidential and will not be used for any purpose other than that for which it is given;
- Of what information is kept about him/her, why it is collected, kept and who has access to it;
- That DRAS only collects/ releases client information that is (a) directly relevant to the provision of its services concerning a specific identified issue and (b) to comply with the Association's duty of care responsibilities;
- Of how the client can get access to the information;

- Of what the main consequences, if any, are for the person if they do not provide the information; and
- Of whom the information might be given to and under what circumstances.

10. CLIENT INFORMATION ACCESS & RELEASE CONSENT

10.1 DRAS will not discuss a client's issues and information with any other people/agencies without the client's written permission. This written permission is documented on either:

- Client Consent to Access/ Release Information form #IA201:2 (a)) or
- Client Consent to Access/ Release Information form #IA201:2 (b).

10.2 Written consent is required before documents about a client can be given to other people/agencies, including people claiming to be a client's representative.

10.3 Authorised discussions about a client will be limited to achieving a client's specified goal(s).

10.4 Where required an accredited interpreter will be used to explain the consent form in the client's preferred language. This will be noted on the form together with the name of the interpreter and the agency the interpreter came from.

10.5 Information will only be sought from agencies or other people specified in the signed Consent to Access and Release Information form.

10.6 The consent form will identify:

(a) the client has authorises DRAS employees (Form #IA201:2(a)) or a specific DRAS employee (Form #IA201:2(b)) to act on their behalf;
(b) information the client authorises to be released/obtained;
(c) agencies/ individuals that will be contacted;
(d) date the authority expires and that if the case is closed before this date, then the authorisation becomes null and void;
(e) validity of a photocopy of the consent form is considered effective and as valid as the original;
(f) right of the client to change or cancel their authority at any time; and
(g) signatures of the client, a relative/friend of client and the DRAS employee.

10.7 Where a client chooses only to authorise a specific DRAS employee to access or release their personal information then Form #IA201:2(b) must be used. The employee will inform the client that this may result in a potential delay should an alternative DRAS employee be required to follow through with the client's case. In such circumstances the client would be required to

sign a new consent form before the alternative DRAS employee could proceed with the client's case. Where a client chooses only to provide consent to a specific DRAS employee this discussion and the potential consequences will be recorded in the client's case notes.

10.8 Before releasing/obtaining any information about a client to any APP entity or person, DRAS employees will explain to the client the reasons why the information is needed.

10.9 Where doubt exists about a person's ability to give informed consent, disclosure of information will be approved by that person's parent, guardian, Attorney under Power of Attorney or a person who has sustained contact with the person with a disability and has demonstrated a genuine concern for that person.

10.10 Identifying information in a client's file must not be used for the purpose of research without written consent from the client.

10.11 The needs and rights of individuals with impaired decision making will be respected through appropriate authorisation processes as required, including:
Children: Where the client is under the age of 12 years parents should generally have access to documents concerning their children.

Where the child is aged between 12-18 years, their wishes should be taken seriously in deciding whether access to their files is reasonable and in their best interest.

Adults: The wishes of adults with a disability should be respected, though it needs to be acknowledged that some clients may not be able to make informed decisions by reason of the degree of their disability:

- access to their personal records by other persons must only be given if based on the client's informed consent; alternatively
- if the client has a disability that impacts on their ability to make decisions, then decision making may reside with family members, carers or a legal guardian.

11. CLIENT RECORDS AND FILE MANAGEMENT

11.1 A hardcopy case file will be created for each new case being represented.

11.2 DRAS will only keep written information such as action plans, case records, case notes, letters, reports, etc. that are relevant to the case.

11.3 Case notes should contain objective information. Care should be taken with the choice of language used.

11.4 All incoming and outgoing correspondence must be dated.

11.5 Case files will not be duplicated, except where sections of a file have been requested by subpoena.

11.6 Files remain the property of DRAS. However, clients have the right, either personally, or through another person that they have nominated to access or seek correction of their personal information in accordance to DRAS' 'Access and Correction of Personal Information' policy (Policy# A106).

11.7 Client files should be kept secure at all times. When ever a case file is to be removed from a DRAS office, including a home office, then the following applies:

- Case files are to be placed in a lockable container (eg lockable brief case, lockable storage box etc.) when removed from the office.
- Case files transported by vehicle are to be securely stored in the boot of the vehicle. If the vehicle does not have a boot (eg station wagon) then the lockable container containing the case file must be securely stored within the vehicle and made inconspicuous,
- Case files that are kept overnight or whilst in transit and will be unattended are to be stored in the employee's house or motel room,
- Case Files that are to be sent by post are to be sent by Registered Post ONLY. An employee must seek and keep an Item Receipt Number until they can verify that the case file has reached its destination and is in the possession of an authorised person,
- The Item Receipt Number must be kept until the employee can verify that the case file has reached its destination and is in the possession of an authorised person,
- Postal and courier details and Item Receipt Numbers are to be recorded in the client's electronic case file.
- Once the employee has verified that a document has reached its destination and is in the possession of an authorised person they are to record this in the client's electronic case file.

11.8 Client records will be kept confidential at all times. The only people who have access to view client information will be DRAS' CEO and relevant employees.

11.9 In accordance with DRAS' Complaints Handling policy (Policy# A402) the DRAS Chairperson and or their delegate may view a client's case file in the event of a client complaint and with the permission of that client.

11.10 DRAS will destroy client's records as follows:
(a) the hard copy of a case file will be destroyed three (3) years after a case has been closed. This will be undertaken in a way that maintains confidentiality (e.g. use of a paper shredder).

(b) the electronic version of a case files will be destroyed six (6) years after the closure of the case.
(c) all other electronic records will be destroyed six (6) years after a client's last contact with DRAS.

11.11 Information that is made available to the public regarding whom DRAS represents will not include any names or addresses.

11.12 As a general principle, DRAS will not keep copies of original client documents eg Centrelink forms.

11.13 The CEO is the only employee to undertake/ authorise the deletion of client information from DRAS' client database.

12. SPECIAL CIRCUMSTANCES

DRAS will release personal information without a client's authority only in a situation where:

(a) DRAS believes that the client is genuinely in serious or imminent danger, presents a danger to others or in an emergency situation, or
(b) Required or permitted by law- such as child protection law.

12.1 Necessity

DRAS will breach confidentiality where an employee reasonably believes that the use of disclosure is necessary to prevent a serious and imminent threat to the individual's life, health or safety or, a serious threat to public health or safety.

A decision to disclose information to help or protect a client will pay due regard to the particular client's capacity to make decisions.

If an employee reasonably believes that they need to disclose client information on the basis of necessity this should be discussed with DRAS' CEO, wherever possible.

12.2 Subpoena

If a client's file is ordered by a subpoena (court/ tribunal order), the client will be notified as soon as possible. Only information ordered by subpoena will be released. In this instance, the information may be photocopied.

12.3 Mandatory Reporting Requirements

DRAS employees may be required by legislation to disclose relevant client information to the relevant authorities if an employee has reasonable grounds to suspect that a child is at risk of harm and that those grounds arise during the course of that employee's work.

13. MISCELLANEOUS

DRAS will not adopt a government related identifier (eg. tax file number, student number or drivers licence number) of an individual as its own identifier for that individual.

14. CLIENTS WITH KNOWN VIOLENT BEHAVIOUR

DRAS employees have a right to a safe and violence free working environment.

Employees should ask agencies that refer people to them if they know or have a reasonable suspicion that the person being referred to DRAS has violent tendencies.

Likewise, where a client of DRAS is being referred to another agency and a DRAS employee knows or reasonably suspects that that client has violent behaviour, the DRAS employee must exercise their duty of care by informing the employees of the other agency that they should undertake appropriate work precautions in relation to the client being referred.

15. LISTS AND REGISTERS

The following applies to information kept on hardcopy and in electronic format.

15.1 Contact List (CL)

The CEO is responsible for ensuring that a CL is established and securely kept.

The purpose of the CL is to enable DRAS to send clients (who have consented to be on the CL) information that may be of interest to them and to invite them participate in DRAS' activities such as information sessions, client reference group meetings and government consultations (Form# IA104:5).

The CL will be securely and confidentially stored. Authorised access to the CL is available to the CEO and subsequently to relevant employees.

Periodically, the CEO may update the CL so as to delete the consent forms of clients who have ceased to have any contact with DRAS for a period of six (6) years, thus maintaining their privacy.

If the Association is to be dissolved the CEO is responsible, as soon as practicable, for the confidential destruction of the CL.

15.2 Evaluation of DRAS' services

Upon the formal closure of their case clients will be invited to evaluate the service that they received from DRAS by filling in a 'Evaluation of Service' form (Form# IA104:3).

The Evaluation of Service form is to be developed in a manner that maintains client confidentiality. The form will not require the client to state their name, however this will be optional. This will facilitate clients providing an honest and frank response without fear of retribution in providing feedback.

The CEO will keep a register of the Evaluation of Service forms. These forms will be kept for a period of no more than two (2) years and will be subsequently destroyed to maintain respondent confidentiality.

15.3 Complaints Register

DRAS will investigate complaints in a manner that, to the extent possible, maintains people's right to confidentiality.

A register will be kept of complaints, including investigation and resolution processes undertaken. The CEO is responsible for secured and confidential storage of the Complaints Register.

Documentation of complaints will be kept for a period of two (2) years or, at the discretion of the CEO, a record may be kept for as long as deemed necessary in consideration of potential legal matters.

In the event of the Association being dissolved, the last Board will put arrangements in place for the confidential storage of complaints records for a period of six (6) years and for their confidential destruction thereafter.

15.4 Association Membership

DRAS will encourage people with disability, their carers and other stakeholders to become members of the Association.

On behalf of the Board, the CEO is responsible for keeping an up-to-date register of members of the Association. The register is a public document and therefore is available for viewing by any member of the public.

The CEO will, on a periodic basis, destroy the membership forms of people who cease to be members of the Association.

In the event of the Association being dissolved, the last Board will put arrangements in place for the safe storage of the Membership Register for a period of six (6) years and for its confidential destruction thereafter.

16. MEDIA AND PUBLICATIONS

Employees will obtain the written consent of people with disability affected by a situation when promoting the issue publicly.

Employees must enable the person(s) to review and endorse media statements prior to their release.

In addition to this, all media release/ statements will also be vetted by the CEO prior to release to ensure:

- its impact on DRAS:
- the accuracy of the media release;
- the dignity of people with disability is maintained; and
- to the extent possible, it maintains the privacy and confidentiality of clients within the limits of the consent they have provided.

DRAS will seek the written consent of clients for their photograph or other identifying images to be displayed in any DRAS publication (e.g. Annual Report, Poster etc) or other forms of publicly available productions (e.g. videos) . Where the image is of a child or young person written consent is to be sought from that person's family or guardian giving consideration to the wishes of the child or young person concerned.

17. STATISTICS AND CASE STUDIES

DRAS will use statistics and case studies relating to its former and current clients in a manner that maintains their confidentiality and privacy.

DRAS:

- Will gather non-identifiable statistics about service users for the purposes of planning, accountability and service delivery.; and
- May use case studies for the purpose of community education. Case studies will not contain information which would cause a client to be identified (i.e. identifying information may be altered to protect the privacy of the client).

18. CONTACT BY OTHER AGENCIES

If another agency wishes to contact a client, DRAS may either invite the client(s) to contact the agency or obtain consent from the client(s) for DRAS to provide the agency with their contact details.

19. PROFESSIONAL DEVELOPMENT & TRAINING

The CEO, or their nominated delegate, will promulgate this policy at an employee's Induction and periodically thereafter..

The CEO is responsible for ensuring professional development opportunities are made available to employees in relation to areas covered by this policy and the National Privacy Principles.

Training attended by DRAS' employees relating to this policy may be recorded in the Professional Development Register and may be reported in DRAS' Annual Report.

20. COMPLAINTS

Any complaints emerging from a breach of confidentiality and privacy should be dealt with according to DRAS' Complaints Handling policy (Policy# A402).

21. LEGAL ADVICE

At any stage, the Privacy Officer may seek legal or professional advice. The cost of such advice will be borne by DRAS.

22. PROMOTION OF THIS POLICY

People accessing DRAS' services will be provided a copy of the Client Induction Booklet, which informs them of the key elements of this policy in an easy to read language format. Alternatively, this policy will be explained to people in an age appropriate manner and relevant to their communication preferences.

A copy of this policy in full will be made available free of charge to anyone who requests it.

23. REVIEW OF POLICY

Congruent with DRAS' commitment to quality planning, performance management and continuous improvement (Policy# GM007), this policy will be reviewed on a triennial basis. However, if at any time the legislative, policy or funding environment is so altered that the policy is no longer appropriate in its current form, the policy shall be reviewed immediately and amended accordingly.

Adapted in part from 'Privacy, Dignity & Confidentiality Policy' , of Welfare Rights Centre Inc. (2005), Spina Bifida Association W.A.(2002), Independent Advocacy in the Tropics Inc., Edge Employment Solutions(2005)