



Data Policy

This Policy was last reviewed and updated on:
12th September 2022.
To be reviewed in 6 months.

Table of Contents

| | |
|----------------------------------------------------------------|-----------|
| 1. Eds. Data Policy Statement Overview | 3 |
| 2. Policy Statement Introduction | 4 |
| 3. Policy statement | 5 |
| 4. About this policy | 6 |
| 5. Definition of data protection terms | 6 |
| 6. Data Protection Officer | 7 |
| 7. Data protection principles | 7 |
| 8. Fair and lawful processing | 8 |
| 10. Notifying data subjects | 11 |
| 11. Adequate, relevant and non-excessive processing | 12 |
| 12. Accurate data | 12 |
| 13. Timely processing | 12 |
| 14. Processing in line with data subject's rights | 13 |
| 15. Data security | 16 |
| 16. Data Protection Impact Assessments | 17 |
| 17. Disclosure and sharing of personal information | 18 |
| 18. Data Processors | 18 |
| 19. Images and Videos | 19 |
| 20. Disclosure of personal information to third parties | 20 |
| 21. Changes to this policy | 20 |
| 22. ANNEX - DEFINITIONS | 20 |

1. Eds. Data Policy Statement Overview

The Eds. Data policy is underpinned by the Privacy Act 1988 protects an individual's personal information regardless of their age and the Health Records and Information Privacy Act 2002 (HRIPA), which require us to comply with Information and Health Privacy Principles.

Storage - AWS server (Australia Based). API to Tableau

Multi - Authentication (Tableau + AWS server).

Persons with access to data: Catriona Fleet, Rebecca Mawdsley, Jessica Swadling and David Carlton (Nominated ASPECT Exec).

Data is identified unless the purpose of data visualisation is to specifically identify the student and the interventions needed to improve that student's life outcomes.

Use student identifiers where possible (rather than names and DOB).

Eds will need a copy of student identifier linked to names and DOB on AWS server but will only be used to answer direct questions of the Executive.

We aim to promote a strong privacy culture by:

- Complying with the requirements of PPIPA and HRIPA;
- Providing privacy awareness training to our staff;
- Continuously improving privacy management; and
- Regularly updating our Privacy Management Plan.

This policy applies to all employees, including permanent, temporary, casual, and contractors and consultants.

1.1 What personal information do we collect?

The personal information we collect about you depends on the nature of your dealings with us or what you choose to share with us.

The personal information we collect about you may include:

- Name
- Mailing or street address
- Date of birth
- Email address
- Phone number
- Class (Class year)
- Previous school (if appropriate)
- Profession
- Academic Records
- Occupational Therapist Reports
- Cognitive Assessments
- Speech Therapist Reports
- Behavioural Therapist Report
- Identifying names (if any)

2. Policy Statement Introduction

NSW privacy legislation focuses largely on information about you, that is, information that identifies you. In NSW, the Acts address two groups of information – personal information and health information.

The Privacy and Personal Information Protection Act 1998 (PPIP Act) protects your privacy rights in NSW by making sure that your personal information is properly collected, stored, used or released by NSW public sector agencies via the Information Protection Principles (IPPs). It states that you have the right to see and ask for changes to be made to your personal or health information. In addition to this, it allows you to make a complaint to the NSW Privacy Commissioner if you believe a NSW public sector agency has misused your personal information or breached one of the IPPs.

Eds. will protect and maintain a balance between data protection rights in accordance with the Privacy and Personal Information Protection Act 1998 (PPIP Act). This policy sets out how we handle the personal data of our young adults, parents, suppliers, employees, workers and other third parties.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All employees are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be deemed as severe misconduct and will be treated as a disciplinary offence, which may result in disciplinary action dependent of the seriousness of the breach.

3. Policy statement

Eds values and respects the privacy of the people we deal with. Eds is committed to protecting your privacy and complying with the Privacy Act 1988 (Cth) (**Privacy Act**) and other applicable privacy laws and regulations.

3.1 Eds values and respects the privacy of others and agrees that everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a post-school program, we will collect, store and process personal data about our young adults, workforce, parents and others. This makes us a data controller in relation to personal data.

3.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.

3.3 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

3.4 All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action dependent on the severity of the data breach.

3.5 The client will choose whether their data is stored using AWS or Google Drive.

4. About this policy

4.1 The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in The Privacy and Personal Information Protection Act 1998 (PIPP).

4.2 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

4.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

4.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

5. Definition of data protection terms

5.1 All defined terms in this policy are indicated in bold text, and a list of definitions is included in the Annex to this policy.

6. Data Protection Officer

6.1 As an educational consultancy, we are required to appoint a Data Protection Officer (“DPO”). Our DPO is Miss Catriona Fleet and they can be contacted at hello@edschange.com

6.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

6.3 The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection

7. Data protection principles

7.1 Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

7.1.1 Processed fairly and lawfully and transparently in relation to the data subject;

7.1.2 Processed for specified, lawful purposes and in a way, which is not incompatible with those purposes;

7.1.3 Adequate, relevant and not excessive for the purpose;

7.1.4 Accurate and up to date;

7.1.5 Not kept for any longer than is necessary for the purpose; and

7.1.6 Processed securely using appropriate technical and organisational measures.

7.2 Personal Data must also:

7.2.1 Be processed in line with data subjects' rights;

7.2.2 Not be transferred to people or organisations situated in other countries without adequate protection.

7.3 We will comply with these principles in relation to any processing of personal data by Eds.

8. Fair and lawful processing

8.1 Data Protection Legislation in NSW (PPIP Act) is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

8.2 For personal data to be processed fairly, data subjects must be made aware:

8.2.1 That the personal data is being processed;

8.2.2 Why the personal data is being processed;

8.2.3 What the lawful basis is for that processing (see below);

8.2.4 Whether the personal data will be shared, and if so with whom;

8.2.5 The period for which the personal data will be held;

8.2.6 The existence of the data subject's rights in relation to the processing of that personal data; and

8.2.7 The right of the data subject to raise a complaint with the Australian Information Commissioner's Office in relation to any processing.

8.3 We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.

8.4 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

8.4.1 Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;

8.4.2 Where the processing is necessary to comply with a legal obligation that we are subject to;

8.4.3 Where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest; and

8.4.4 Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

8.5 When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

8.5.1 Where the processing is necessary for employment law purposes, for example in relation to sickness absence;

8.5.2 Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

8.5.3 Where the processing is necessary for health or social care purposes, for example in relation to young adults with medical conditions or disabilities; and

8.5.4 Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

8.6 We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a young adult joins us.

8.7 If any data user is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

Vital Interests

8.8 There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

8.9 Where none of the other bases for processing set out above apply then Eds must seek the consent of the data subject before processing any personal data for any purpose.

8.10 There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

8.11 When pupils and or our workforce join the team at Eds, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

8.12 We will generally seek consent directly from a young adult who has reached the age of 14 (Year 9 and above); however, we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

8.13 If consent is required for any other processing of personal data of any data subject then the form of this consent must:

8.13.1 Inform the data subject of exactly what we intend to do with their personal data;

8.14.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

8.14.3 Inform the data subject of how they can withdraw their consent. **8.15** Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

8.14 The DPO must always be consulted in relation to any consent form before consent is obtained.

8.15 A record must always be kept of any consent, including how it was obtained and when.

9. Processing for limited purposes

9.1 In the course of our activities as an educational post-school program, we may collect and process the personal data set out in our Schedule of Processing Activities. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other programs, parents, other young adults or members of our workforce).

9.2 We will only process personal data for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject. (Record data of employees online with consent and in line with protection legislation)

10. Notifying data subjects

10.1 If we collect personal data directly from data subjects, we will inform them about:

10.1.1 Our identity and contact details as Data Controller and those of the DPO;

10.1.2 The purpose or purposes and legal basis for which we intend to process that personal data;

10.1.3 The types of third parties, if any, with which we will share or to which we will disclose that personal data;

10.1.4 Whether the personal data will be transferred outside the NSW Government and if so the safeguards in place;

10.1.5 The period for which their personal data will be stored;

10.1.6 The existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and

10.1.7 The rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

10.2 Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible thereafter, informing them of where the personal data was obtained from.

11. Adequate, relevant and non-excessive processing

11.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

12. Accurate data

12.1 We will ensure that personal data we hold is accurate and kept up to date.

12.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

12.3 Data subjects have a right to have any inaccurate personal data rectified. See further below in relation to the exercise of this right.

13. Timely processing

13.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

14. Processing in line with data subject's rights

14.1 We will process all personal data in line with data subjects' rights, in particular their right to:

- 14.1.1** Request access to any personal data we hold about them;
- 14.1.2** Object to the processing of their personal data, including the right to object to direct marketing;
- 14.1.3** Have inaccurate or incomplete personal data about them rectified;
- 14.1.4** Restrict processing of their personal data;
- 14.1.5** Have personal data we hold about them erased
- 14.1.6** Have their personal data transferred; and
- 14.1.7** Object to the making of decisions about them by automated means.

The Right of Access to Personal Data

14.2 Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with Eds Subject Access Request Procedure.

14.3 In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

14.4 An objection to processing does not have to be complied with where Eds can demonstrate compelling legitimate grounds which override the rights of the data subject.

14.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

14.6 In respect of direct marketing any objection to processing must be complied with.

14.7 Eds is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

14.8 If a data subject informs Eds that personal data held about them by Eds is inaccurate or incomplete then we will consider that request and provide a response within one month.

14.9 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the data subject within one month of their request that this is the case.

14.10 We may determine that any changes proposed by the data subject should not be made. If this is the case then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the Australian Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

14.11 Data subjects have a right to "block" or suppress the processing of personal data. This means that Eds can continue to hold the personal data but not do anything else with it.

14.12 Eds must restrict the processing of personal data:

14.12.1 Where it is in the process of considering a request for personal data to be rectified (see above);

14.12.2 Where Eds is in the process of considering an objection to processing by a data subject;

14.12.3 Where the processing is unlawful but the data subject has asked Eds not to delete the personal data; and

14.12.4 Where Eds no longer needs the personal data but the data subject has asked Eds not to delete the personal data because they need it in relation to a legal claim, including any potential claim against Eds.

14.13 If Eds has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

14.14 The DPO must be consulted in relation to requests under this right.

14.15 Data subjects have a right to have personal data about them held by Eds erased only in the following circumstances:

4.15.1 Where the personal data is no longer necessary for the purpose for which it was originally collected;

14.15.2 When a data subject withdraws consent – which will apply only where Eds is relying on the individuals consent to the processing in the first place;

14.15.3 When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object;

14.15.4 Where the processing of the personal data is otherwise unlawful;

14.15.5 When it is necessary to erase the personal data to comply with a legal obligation;

14.16 Eds is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

14.16.1 To exercise the right of freedom of expression or information;

14.16.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

14.16.3 For public health purposes in the public interest;

14.16.4 For archiving purposes in the public interest, research or statistical purposes; or

14.16.5 In relation to a legal claim.

14.17 If Eds has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

14.18 The DPO must be consulted in relation to requests under this right.

14.19 In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to other organisation.

14.20 If such a request is made then the DPO must be consulted.

15.Data security

15.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

15.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

15.3 Security procedures include:

15.3.1 Entry controls. Any stranger seen in entry-controlled areas should be reported to the Director of Finance & Resources.

15.3.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).

15.3.3 Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required and use of such devices discouraged. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

15.3.4 Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

15.3.5 Working away from Eds premises – paper documents. Documents containing personal information should not be taken away from the Eds premises.

15.3.6 Working away from Eds premises – electronic working. Eds has remote access for all employees to facilitate working away from the Eds premises.

15.3.7 Document printing. Documents containing personal data must be collected immediately from printers and not left on photocopiers.

15.4 Any employee found to be in breach of the above security measures may be subject to disciplinary action.

16. Data Protection Impact Assessments

16.1 Eds takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

16.2 In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

16.3 Eds will complete an assessment of any such proposed processing which ensures that all relevant matters are considered in relation to the DPIA.

16.4 The DPO should always be consulted as to whether a data protection impact assessment (DPIA) is required, and if so how to undertake that assessment.

17. Disclosure and sharing of personal information

17.1 We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education NSW [Health authorities and professionals, the Local Authority (The Office of Local Government), the NDIS and other organisations where we have a lawful basis for doing so.

17.2 Eds will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

17.3 In some circumstances we will not share safeguarding information.

17.4 Further detail is provided in our Schedule of Processing Activities.

18. Data Processors

18.1 We contract with third party organisations (only on a needs must basis and we will seek permission from the client prior to engaging these companies):

18.1.1 Studio LDN for data dashboards;

18.1.2 Hello Again for data dashboards;

18.2 In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

18.3 Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of Eds. Eds will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

18.4 Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

19. Images and Videos

19.1 Parents and others attending Eds events are allowed to take photographs and videos of those events for domestic purposes. For example, parents/carers can take video recordings of a Eds performance involving their young adult. Eds does not prohibit this as a matter of policy.

19.2 Eds does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of Eds to prevent.

19.3 Eds asks that parents and others do not post any images or videos which include any child/young adult other than their own child/young adult on any social media or otherwise publish those images or videos.

19.4 As educational experts, we want to celebrate the achievements of our participants and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering Eds events or achievements. We will seek the consent of young adults, and their parents/carers where appropriate, before allowing the use of images or videos of pupils for such purposes.

19.5 Whenever a young adult begins their attendance at Eds. they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

20. Disclosure of personal information to third parties

We may disclose your personal information to third parties in accordance with this policy in circumstances where you would reasonably expect us to disclose your information. For example, we may disclose your personal information to:

- Studio LDN
- Hello Again
- Our marketing providers
- Our professional services advisors

21. Changes to this policy

21.1 We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

22. ANNEX - DEFINITIONS

| Term | Definition |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data | is information which is stored electronically, on a computer, or in certain paper-based filing systems |
| Data Subjects | for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be an Australian Citizen. All data subjects have legal rights in relation to their personal |

| | |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | information |
| Personal Data | <p>means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person</p> <p>Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.</p> |
| Data Controllers | <p>are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation.</p> <p>We are the data controller of all personal data used in our business for our own commercial purposes</p> |
| Data Users | are those of our employees whose work |

| | |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times |
| Data Processors | include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions |
| Processing | is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties |
| Special Category Personal Data | includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data |
| Workforce | Includes, any individual employed by |

| | |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Academy such as staff and those who volunteer in any capacity including Governors and/or Trustees / Members/ parent helpers |
| HRIPA - Health Records and Information Privacy Act 2002 (NSW) | The Act allows for individuals to obtain access to health information and establishes a framework for the resolution of complaints regarding the handling of health information. |
| PPIPA Privacy and Personal Information Protection Act 1998 | The Privacy and Personal Information Protection Act 1998 (PIIP Act) outlines how New South Wales (NSW) public sector agencies manage personal information and the functions of the NSW Privacy Commissioner. |
| ICO | Information Commissioner's Office |
| PC - The Information and Privacy Commission NSW | An independent authority that administers legislation dealing with privacy and access to government held information in New South Wales |
| DPIA - A Data Protection Impact Assessment | Describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with data protection |

| | |
|--|--------------|
| | legislation. |
|--|--------------|