PRIVACY POLICY

References

1. The National Privacy Principles in the Privacy Amendment (Private Sector) Act 2000
2. The Privacy Act 1988
3. Workers Compensation and Rehabilitation Act QLD 2003
4. Axiom College Information Technology Security Policy (POL14)

Definitions

Non-profit Organisation	means: a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.
Employee Record	means: a record of personal information relating to the employment of an employee. It includes health information about an employee and personal information.
Personal Information	means: information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about a client whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Sensitive information	means information or an opinion about a client'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 or trade union, sexual preferences or practices, criminal record, health information about a client.
Health Information	means information or an opinion about: the health or disability (at any time) of a client, a client's expressed wishes about the future provision of health services to him or her, a health service provided, or to be provided, to a client that is also personal information.
Record	means: a document, a database (however kept), a photograph or other pictorial representation of a person.
Unlawful Activity	means: acts or omissions that are expressly prohibited by Commonwealth, State and Territory law.
Government Contract	means:

	a Commonwealth contract or a State contract.
Law	means: Commonwealth, State and Territory Legislation, as well as Common law.
Required by Law	means: that an organisation must deny access to personal information.
Authorised by Law	means: a law that gives an organisation the discretion to deny access to personal information.
Identifier	means: a number assigned by an organisation to a client to identify uniquely the client for the purposes of the organisation's operations.

1. Overview of the Private Sector Provisions of the Privacy Act 1988

The private sector provisions in the Privacy Act 1988 ((Cth) regulate the way in which Axiom College collect, use, keep secure and disclose personal information. It gives clients the right to know what information we hold about them and a right to ensure that their information is corrected if it is wrong. The private sector provisions aim to give people greater control over the way information about them is handled in the private sector and ensures compliance by organisations with the ten National Privacy Principles (These may be viewed by contacting the Axiom College Quality Officer or can be found at the Federal Privacy Commissioner Website: www.privacy.gov.au).

Axiom Collegemust take reasonable steps to make clients aware that it is collecting personal information about them, the purposes for which it is collecting the information, and who it might pass the information on to. There are some restrictions on the uses we can make of personal information and when we can disclose personal information or transfer it overseas. Axiom College must not collect personal information unless the information is necessary for one or more of our functions or activities and only by lawful and fair means and not in an unreasonably intrusive way.

Except for some special circumstances, clients have a right to get access to personal information we hold about them and to have the information corrected or annotated if the information is incorrect, out-of-date or incomplete. Clients can also make a complaint if they think information about them is not being handled properly.

2. Purpose of this Policy and Procedures

The purpose of this policy is to offer information and guidance to Axiom College staff and clients regarding the obligations under the ten National Privacy Principles. This Policy is to make up part of the staff induction process and is to be made feely available to any person requesting it.

3. Appointment of Privacy Officer

The Managing Director is authorised to appoint a Privacy Officer to ensure that Axiom College has a first point of contact when privacy issues arise either internally or from outside the company. The privacy officer's responsibilities include:

- action any privacy matters which cannot be resolved through normal business practice
- offering advice to management, staff and clients on matters pertaining to privacy
- ensuring that Axiom College's Privacy Policy and Procedures are fully implemented, maintained and the plan promoted to all relevant parties
- expediently and openly deals with client complaints regarding privacy matters

- ensuring that the Axiom College complies with the relevant law

4. Anonymity

Persons entering into transactions with Axiom College have the option not to identify themselves when entering into those transactions. Should this occur staff should point out to the person concerned that this may have an adverse effect on our capacity to offer the full range of our services to them.

5. Openness

National Privacy Principles state that we are to be open about our handling of personal information. Our documentation (where applicable) contains relevant privacy information for the information of our clients. Upon request by a client, staff are to take reasonable steps to let people know:

- what sort of personal information we hold
- for what purpose we hold the information
- how the information is collected
- how we store and use the information
- who the information is disclosed to (where applicable)

6. What Type of Information May a Client Ask For?

The information people may request will be subject to their requirements. Some of the types of information that may be requested include:

- the kind of personal information Axiom College collects about them
- what, if any, of that information is sensitive information under the Privacy Act 1988
- the purposes for which Axiom College collects or holds personal information
- the kinds of personal information the organisation shares with related agencies or companies
- more information about who the organisation discloses personal information to and the reasons for doing so
- details of the Axiom College's functions or activities that involve personal information and are contracted out
- who the person can contact at Axiom College if they have a privacy concern
- Axiom College contact details, for example, the name, street and postal addresses, the main telephone and fax numbers and appropriate e-mail addresses (these details are contained within the headers of our documents as part of our normal business practice)
- how we at Axiom College store and secure our information (you are not to release specific details of security measures that would jeopardise the security of any personal information)
- how clients are able to get access to information Axiom College holds about them
- the kinds of personal information Axiom College may transfer overseas
- how a client can make a complaint to Axiom College about a possible breach of privacy, including, the contact number for our Grievance Officer

7. Client Reasons for a Request for Access to Personal Information

Clients do not have to give a reason for the request for access to their information. Staff should question the client to ascertain the exact type and amount of information they request.

8. Factors Effecting the Way We Present Information

When we become aware of any particular requirements affecting a client requesting information we should consider presenting the information in a way that takes into account those requirements. Some factors that may affect the way we present information could include:

- any disability the client may have
- the client's level of understanding
- the client's language or literacy skills

9. Reasonable Steps when Providing Information

We are required when requested, to take reasonable steps to let a client know, what sort of personal information we hold, for what purposes and how we collect, use and disclose the information. The National Privacy Principles do not limit the type or detail of information that we may provide. We may tailor the information according to what the client wants to know. Axiom College staff are to consider a number of matters when deciding what are reasonable steps when providing information to our clients, including:

- the complexity of the information we hold, for example, if the request is a simple one such as the date and time of a previous appointment, then it would be appropriate to give the information verbally
- for more complex requests for information for example, the request may be an entire history of the persons apprenticeship or traineeship then written material may be a better option
- how much information the client wants, when providing information, whether simple or complex, it is to be presented in a user-friendly, accessible way and avoid jargon or in-house terms.

10. Access and Correction of Personal Information

10.1 Charges for Access to Information

Under principle 6 of the National Privacy Principles we may not charge a fee to a person to lodge a request for access to information. Axiom College may apply a fee for the recovery of costs only for making the information available. Costs are to be considered on a case-by-case basis. When assessing how much to charge a client for access, the following will need to be considered:

- staff costs involved in the locating and collating of the information
- costs to reproduce the information
- costs associated with explaining the information to someone
- costs associated with the employment of intermediaries either at company expense or shared between Axiom College and the client
- charges are not to exceed the cost to the company to process the request
- waiving or remitting the cost particularly where a client is in receipt of a Government benefit or pension.

10.2 Factors Affecting Access

The way Axiom College provides a client with access to their personal information could be affected by various factors including:

- the sort of information the client has asked for access to
- the way the client made the request
- the way we store the information
- the technology the client making the request has access to (e.g. E-Mail)
- the location of the client making the request
- any exceptions that apply to the information requested

10.3 Ways of Giving Clients Access to Information About Themselves

Examples of the way we could give access include:

- letting the client inspect all the information the organisation holds about him or her
- provide a photocopy of the information and let the client take away copies
- let the client take notes of the contents of the record
- give the client a printout of the information if it is in electronic form
- let the client view the information and have a suitably qualified person explain the contents
- fax or e-mail the information asked for to the client
- give the client an accurate summary of the information

10.4 Steps to Correct Personal Information

Should we hold personal information about a client and the information is found (or the client is able to establish) that the information is not accurate, complete and up-to-date, all reasonable steps to correct the information must be taken as soon as practicable after the discovery of the inaccuracy.

10.5 Form of Request for Access to Information

There are two ways that Axiom College are to receive requests for information, they are:

- verbally over the phone or in person for requests of a simple nature
- in writing (in a letter, fax or e-mail) for requests of a more complex nature

11. Establish the Clients Identity

There is a risk that someone may try to access another person's information either by mail, phone, fax, e-mail or in person. Personal information is not to be disclosed to any person other than the person the information directly refers to. Only when the positive identity of the client is confirmed is the information to be released. The identity of the person requesting the information is to be positively established by using the following methods:

Method of Request	Method of Verification of Identification
Telephone	Request the person requesting access to verify at least two of the following and confirm the source of identity: • Next of Kin Information • Job Seeker Number (If applicable) • Tax File Number • Drivers Licence Number
Fax/E-Mail or Surface Mail	Verify the source of the correspondence. Contact the person requesting access by telephone and verify as per telephone above.
In Person	If the person requesting the access is known begin the access process. If the person is not known, have the person present photo I.D. e.g. Drivers Licence, or have the person verify their I.D. by following the process as per telephone above.

Note: If the identification of the person requesting the access to information cannot be verified the request is to be denied, the client informed of the decision as stated in paragraph 12 and the request forwarded to the Privacy Officer for further action.

12. Explaining to the Client the Reasons for Denial of Access or Refusal to Correct Personal Information

If a request for information or correction of personal information is refused the client must be informed of the reasons for denying access to or correction of the information. The reasons for the denial or refusal are to be provided to the person in writing, stating the reasons for the refusal and a copy of the reasons held with the document/s. The written reasons are only to be released subject to approval by the Privacy Officer. Reasons for putting this information in writing include:

- it gives Axiom College an accountability trail in the event of a complaint
- it will help the client to understand the reasons given by Axiom College and so help to avoid unnecessary complaints

12.1 Additional Considerations

When informing the client of the reasons for denying access or refusing to correct information, the person giving the reasons should consider including information about:

- Axiom College's process for reviewing the decision
- the process the client can follow if they wish to make a complaint about the decision either through the Axiom process or to the Federal Privacy Commissioner (Staff are to guide the client towards the Axiom College complaints process in the first instance)

13. Giving an Explanation to a Client Instead of Access to Evaluative Information

National Privacy Principle 6 allows Axiom College not to release information that will reveal the formulae, or the fine details of the evaluative process we use in our commercially sensitive business decisions but it is not aimed at preventing the release of the result of the information nor the factual information about the client.

The person requesting the information is to be given access only to the raw information and the opinions that were used in the evaluation process and an explanation of any decision based on the evaluative process.

14. Providing an area for Inspection of Information

Where feasible consideration should be given to providing a private and convenient area where the client can inspect the information requested or where the client can have the information explained to them. Reasons for considering providing such an area are:

- that it is not appropriate to explain the contents of an client's personal information (in particular, health information) in a busy, open public space such as a reception counter
- that it would not ordinarily be reasonable to expect people to inspect large quantities of information, which may take a long time to go through, while standing at a public counter

15. Use of Intermediaries when the Client is Accessing Information

National Privacy Principle 6 requires that Axiom College consider using intermediaries to allow our clients to gain access to personal information that would otherwise be denied by having an intermediary explain the information to the client.

15.1 Role of the Intermediary

An intermediary is a person or persons acceptable to both Axiom College and the client asking for access to personal information. The role of the intermediary is to
enable a client to gain access to and have the contents of the personal information explained to them, that would otherwise have been denied to them.

15.2 Type of Information Explained by an Intermediary

The type of information explained by the intermediary depends on the instructions given to him/her by the Managing Director, General Manager or the Privacy Officer.

15.3 Considerations before Using an Intermediary

Before using intermediaries in the access process consideration should be given to the following:

- giving access to the client but block out information which has been deemed to be excluded
- give the person a summary of the information and exclude the information which is required to be excluded
- explore any other way in which the requirements of the client and Axiom College can be satisfied

15.4 Steps When Using an Intermediary

It is up to Axiom College management to make the decision when an intermediary is to be engaged. Factors may include the kind of relationship the organisation has with the client,

the exception that will deny the client direct access and the sensitivity of the information requested. The following steps should be followed:

- notify the client of the decision to use an intermediary. This is to be done either verbally or in writing, stating the exception that prevents direct access and suggesting the use of an intermediary who is mutually acceptable to both parties.
- explain in an easily understood way the role of the intermediary
- how the procedure is to work
- explain any costs that the client will incur if an intermediary is used
- explain what the client needs to do next

16. Activities Related to Government Contracts

The Privacy Act exempts the acts and practices of contracted service providers for a Government contract when those acts or practices are directly or indirectly related to meeting obligations under the contract. This statement does not exempt Axiom College from maintaining vigilance in the security of the personal information we collect and store within Axiom College.

17. Security of Personal Information

All staff are to ensure that the personal information they collect, use or disclose is accurate, complete and up to date.

17.1 Staff must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed. National Privacy Principle 2 should be read in conjunction with this paragraph. Staff are reminded that the integrity of normal business practices associated with archiving and storage of Administrative and Trainee files is to be maintained.

18. Unlawful Activity and Law Enforcement

18.1 Unlawful Activity Disclosure

The Privacy Act 1988 seeks to balance client privacy with the public interest in law enforcement and Government Regulation. National Privacy Principle 2 allows Axiom College to use or disclose personal information when there is reason to suspect that unlawful activity has been is being or may be engaged in. National Privacy Principle 2.1 should be read in conjunction with this paragraph. When unlawful activity is suspected it must be based on fact. The suspected unlawful activity will ordinarily relate to the operations of Axiom College.

18.2 Disclosure Required by Law

There maybe times when Axiom College is required by law to use or disclose personal information in a particular way. Some examples are:

- a warrant, order or notice issued by a Court or Government agency for the provision of information, or the production of books, records, or documents held by us for inspection
- statutory requirements to report matters to agencies or enforcement bodies such as:
  - the reporting of specific financial transactions to Austrac
  - the reporting of notifiable accidents, injury or dangerous occurrences to Workplace Health and Safety authorities
- legislation that requires an organisation to carry out some action, which of necessity involves particular uses or disclosures of personal information.

18.3 Other Areas of Use and Disclosure under National Privacy Principle 2

All staff are encouraged to read the Private Sector Information Sheet No: 7 – 2001 'Unlawful Activity and Law Enforcement' available from Office of the Australian Information Commissioner (OIAC): www.privacy.gov.au). This information sheet covers additional issues regarding Axiom College dealings with other areas of use and disclosure such as:

- to law enforcement bodies e.g.,DETE Queensland Police Service, Australian Securities and Investments Commission (ASIC)
- the enforcement of criminal law
- laws imposing a penalty or sanction e.g. Workplace Relations or WorkHealth and Safety Legislation
- the protection of public revenue e.g. taxation
- serious improper conduct e.g. corruption, abuse of power, dereliction of duty
- proceedings in a court or tribunal

18.4 Staff Action Upon Request by Law

Should any staff member receive a request requiring disclosure by law such as a warrant, order or notice the request is to be handed to the Privacy Officer who in consultation with the Managing Director is to assess the scope of the request and ensure that only the personal information requested is released. The Managing Director is to be informed of all matters that come under the headings of paragraph 18.3.

19. Contractors

Staff who are responsible for the management of contracts on behalf of Managing Director are to make themselves familiar with the requirements of Private Sector Information Sheet No: 8 – 2001 in order to ensure compliance with the Act.

20. Collecting, Using or Disclosing Health information as Required by Law

Axiom College may collect, use or disclose health information for statistical purposes only relevant to public health or public safety or health service management activities in accordance with National Privacy Principle 2.1(d). Those activities include the management of our personnel in relation to the requirements of the Work Health and Safety Act 2011 Qld and the Workers' Compensation & Rehabilitation Act 2003 or as indicated below:

- the person has consented to the use or disclosure of the information, Axiom College is to use or disclose the information for the same purpose for which the information was collected (see National Privacy Principle 2) Axiom College is using or disclosing the information for a purpose directly related to the primary purpose for which we collected the information and the client would reasonably expect us to use/disclose the information for that purpose

21. Use of Identifiers

21.1 Axiom College must not adopt as its own identifier (e.g. Apprentice /Trainee Identification Number issued by DETE) of a client an identifier of the client that has been assigned by:

- an agency (such asDETE)
- an agent of an agency acting in its capacity as agent such as RTO's
- a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract

21.2 Axiom College must not use or disclose an identifier assigned to a client by an agency, or by an agent or contracted service provider mentioned in paragraph 20.1 above unless:

- the use or disclosure is necessary for the organisation to fulfil its obligations to the agency
- one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure
- the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances under the Privacy act 1988.

Note: A client's name or ABN is not classed as an identifier.

22. Transborder Data Flow

Axiom College may transfer personal information about a client to someone (other than the organisation or the client) who is in a foreign country only if:

- Axiom College believes that the recipient of the information is subject to a law or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles
- the client consents to the transfer
- the transfer is necessary for the performance of a contract between the client and the organisation, or for the implementation of pre-contractual measures taken in response to the client's request
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the client between Axiom College and a third party
- all of the following apply:
    - the transfer is for the benefit of the client
    - it is impracticable to obtain the consent of the client to transfer the information
    - if it were practicable to obtain consent, the client would be likely to give it
- Axiom College must take 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 National Privacy Principles.

23. Employee Records

Generally, employee records are exempt from the provisions of the National Privacy Principles however, private Sector Information Sheet No: 12 – 'Coverage of the Exemptions from the Private Sector Provisions' should be read to clarify specific issues related to employee records.

24. Complaints Handling

Due to the sometimes complex nature of client complaints regarding the disclosure of personal information all formal client complaints (either verbal or written) are to be directed to the Privacy Officer who is to investigate the circumstances of the complaint and make recommendations to the Managing Director or General Manager of the courses of action open to both the client and management on a case by case basis. This process is to be handled in a sensitive and open manner having regard for the requirements of all parties involved under the National Privacy Principles.

25. Information Held Prior to Commencement of the Private Sector Amendments

Not all of the National Privacy Principles apply to personal information that Axiom College has already collected at the time the private sector provisions came into effect. The table over the page sets out whether the National Privacy Principles applies to information already collected and when each National Privacy Principle will apply.

National Privacy Principle	Topic	What information the National Privacy Principle applies to
NPP 1	Collection	only applies to information collected after 21 December 2001
NPP 2	Use and disclosure	only applies to information collected after 21 December 2001
NPP 3	Data quality and collection	as it applies to collection it only applies to information collected after 21 December 2001
NPP 3	Data quality on use and disclosure	as it applies to use and disclosure it applies regardless of when it was collected
NPP 4	Data security	applies regardless of when information was collected
NPP 5	Privacy policies and openness	applies regardless of when information was collected
NPP 6	Access and correction	if information already held is not used or disclosed it only applies to information collected after 21 December 2001, But if information already held is used or disclosed after commencement then rights of access and correction apply unless: • there is an unreasonable administrative burden; or it will cause the organisation unreasonable expense.
NPP 7	Commonwealth Government identifiers	applies regardless of when information is collected
NPP 8	Anonymity	only applies to information collected after 21 December 2001
NPP 9	Transborder data flow	applies regardless of when information collected
NPP 10	Collection of sensitive information	only applies to information collected after 21 December 2001

26. Review of this Document

This Policy Document is to be reviewed annually as part of the normal review process or at any other time as governed by Axiom College or statutory requirement.