MWLP PRIVACY POLICY

MWLP works with local committees, coordinators and staff, organisations and other stakeholders in the provision of a quality service that supports the school to work transition for students in the Macarthur and the greater Bankstown areas.

To this end we ensure that we safeguard the information that we have obtained through our day-to-day operations.

MWLP, in our commitment for quality and service to our stakeholders is working to the National Privacy Principles (NPPs) and Information Privacy Principles (IPPs). These privacy principles are set out in the Privacy Act 1988.

To comply with our obligations under the NPPs and IPPs, this privacy policy sets out how MWLP manages information, about our individual stakeholders, in our organisation.

MWLP will:

- Only request personal information that is pertinent to the provision of program requirements
- Ensure the privacy and security of the information that we receive, in our files and databases.
- Not divulge personal information to third parties without prior consent.
- Ensure that our committee members, staff, sub contractors, work experience or workplacement students adhere to Macarthur Workplace Learning Program Inc. Privacy Policy.
- MWLP will monitor and audit the Privacy Policy to ensure that all requirements are met, and provide training programs to ensure that all persons with access to our information comply and understand these requirements.

30th November 2002

PERSONAL INFORMATION COLLECTION STATEMENT

Your personal information

MWLP will collect your personal information for the purposes of work placement, employment, traineeships, apprenticeships and follow up surveys as required.

Personal information is any information or an opinion about you.

It could include the opinions of others about work placement performance and other information obtained by us in connection with work placements.

This information is subject to the Privacy Act 1988 and the Privacy Amendments Private Sector 2002

How your information will be collected

Personal and sensitive information will be collected from you directly when you fill out and submit one of our information forms with supporting documents or any other information in connection with your workplacement arrangements.

Personal and sensitive information will also be collected from workplacement checks and inquiries to employers, school/TAFE and education bodies.

It will also come from the results of workplace performance feedback/comments from you or about you.

Your information will be used

Your personal and sensitive information may be used in connection with work placement, performance appraisals and the assessment of placement.

This information may also be used for follow up surveys as required.

Disclosing of your personal and sensitive information

Your personal and sensitive information may be disclosed to workplacement employers and education bodies as part of our arranging workplacements.

We may also disclose information to a government body that has a proper interest in the disclosure of your information and any person with a lawful entitlement to obtain the information.

How long will your information be retained?

The information will be stored securely and be retained until the student reaches the age of 21 years or 3 years after the placement has been completed, whichever is longer.

INFORMATION PRIVACY PRINCIPLES

This Code of Practice is consistent with the Information Privacy Principles (IPPs), endorsed by the NSW Privacy Committee, which may be summarised as follows:

Principle 1: Collection of information must be lawful and fair

Personal information should only be collected for a lawful purpose directly related to a function or activity of the agency.

Principle 2: Informed consent

Personal information should normally be collected directly from the individual concerned. At the time the information is collected the individual should be advised why it is being collected, whether provision of the information is compulsory and who else will have access to the information.

Principle 3: Data quality

Agencies should take reasonable steps to ensure that the personal information they collect is relevant, accurate, up-to-date and complete and does not intrude to an unreasonable extent on the personal affairs of the individual concerned.

Principle 4: Data security

Agencies should ensure that personal information is protected by appropriate security safeguards from loss, unauthorised access or misuse.

Principle 5: Openness

Any person has a right to know whether an agency holds personal information about them and, if so:

- It's nature and source.
- the main purpose for which it is used.
- the classes of persons about whom it is kept.
- the period for which the information is kept.
- the persons who are entitled to have access to it; and
- how to obtain access to it.

Principle 6: Access

A person has a right of access to personal information held by an agency, subject to exceptions of the Freedom of Information Act or other relevant law.

Principle 7: Correction of records

Agencies should make any corrections, deletions or additions to personal information to ensure it is accurate, up-to-date and complete.

Agencies should, on request, add any reasonable statement a person wishes to see included in their record. Other recipients of the information should be informed about corrections.

Principle 8: Ensuring data quality before use

Agencies should take reasonable steps to ensure that information is relevant, accurate, up-to-date and complete before use.

Principle 9: Using personal information

Agencies should not use personal information for purposes other than for which it was collected except:

- with the consent of the person
- to prevent a serious threat to a person's life or health
- as required or authorised by law.

Principle 10: Disclosing personal information

Agencies should not disclose personal information to other parties except:

- with the consent of the person
- to prevent a serious threat to a person's life or health
- as required or authorised by law.

The recipient of the information can only use it for the purpose for which it was disclosed.

Principle 11: Sensitive personal information

Notwithstanding principles 9 and 10, information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life should not be disclosed by an agency without the express written consent, freely given, of the individual concerned, or authorisation under the law.