Privacy Policy

1. INTENT

This Privacy Policy is based on the Australian Privacy Principles (APP) of the *Privacy Act* 1988 (Cth). The guidelines ensure The John Flynn College ("the College") protects resident's and employee's privacy in line with the *Privacy Act* 1988 (Cth) and the Office of the Australian Information Commissioner's (OAIC).

2. PRINCIPLES

Protecting personal information is important to the College and personal information is held in the strictest of confidences.

Personal information will only be used for the purposes it was collected or in the way that the provider has given the College permission to use it.

The APPs set out the standards, rights and obligations of the College in relation to handling, holding, accessing and correcting personal information. The APPs do not apply to de-identified information or statistical data sets which would not allow individuals to be identified.

The privacy of residents and employees of the College is maintained at all times. All employees sign a confidentiality statement on employment which binds them to confidentiality after leaving the organisation.

The Deputy Principal is the College's Privacy Officer and will be responsible for reporting to senior management about privacy issues which include, complaints, data breaches, evaluation processes and any changes to practices.

The Privacy Officer will access training resources from the Office of the Australian Information Commission to provide training to staff to develop and maintain effective privacy practices.

3. POLICY REVIEW

This College will review this Policy regularly in accordance with its policy review process. It may amend the Policy from time to time to ensure its currency with respect to relevant legislation to improve the general effectiveness and operation of the Policy.

4. SCOPE

This policy applies to all residents, volunteers and employees of the College.

5. DEFINITIONS

Authorised User means a staff member or resident who has been provided with an Authentication Credential by the James Cook University to access University IT Services.

Data breach means the loss, unauthorised access to, or disclosure of, personal information.

Employee record means a record of confidential personal information relating to the employment of a staff member. The employee record comprises information about employment, including health, recruitment and selection, terms and conditions of employment, performance, discipline, and resignation. Employee records are exempt from the provisions of the Act.

Loss means accidental or inadvertent loss of personal information likely to result in unauthorised access or disclosure. For example, an employee leaves a copy of a document or a device on public transport. If data can be deleted remotely or is encrypted it will not constitute an NDB.

Privacy Policy

Notifiable Data Breach (NDB) is a data breach that is likely to result in serious harm to any of the individuals to whom the personal information relates. A NDB occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. In such circumstances, the College must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as required under the *Privacy Amendment (Notifiable Data Breaches) Act* 2017

Permitted general situation has the same meaning as provided for in section 16A of the Act and referred to in APP 6.2(c). The permitted general situations are: lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety; taking appropriate action in relation to suspected unlawful activity or serious misconduct; locating a person reported as missing; asserting a legal or equitable claim; conducting an alternative dispute resolution process.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:-

(a) whether the information or opinion is true or not, and
(b) whether the information or opinion is recorded in a material form or not.

Sensitive Information means information or an opinion about an individual's

(a) racial or ethnic origin;
(b) political opinions;
(c) membership of a political association;
(d) religious beliefs or affiliations;
(e) philosophical beliefs;
(f) membership of a professional or trade association;
(g) membership of a trade union;
(h) sexual preferences or practices; or
(i) criminal record.

Serious harm is determined with regard to the following list of relevant matters as provided for in section 26WG of the *Privacy Amendment (Notifiable Data Breaches) Act* 2017:

- the kind or kinds of information;
- the sensitivity of the information;
- whether the information is protected by one or more security measures;
- if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
  - if a security technology or methodology was used in relation to the information; and
  - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;
  - the likelihood that the persons, or the kinds of persons, who have obtained, or who could obtain, the information; and
  - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;
  - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;
- the nature of the harm;
- any other relevant matters.

Unauthorised access means personal information accessed by someone who is not permitted to have access. This could include an employee of the entity, a contractor or external third party (such as hacking).

Unauthorised disclosure means where an entity releases/makes visible the information outside the entity in a way not permitted by the Privacy Act. For example, N employee accidently publishes a confidential data file containing personal information on the internet.

6. POLICY

The APPs protect residents, volunteers and employees of the College. The College Principal is responsible for the protection of the personal information records held by the College and ensures that there is compliance throughout the organisation.

6.1 Types of Personal Information the College collects and holds

The College generally asked for all or some of the following types of personal information:-

From residents:-

- Resident's enrolment details from James Cook University;
- Resident's academic results from James Cook University;
- Title, name, address and contact details;
- Gender;
- Date of Birth;
- Name of next of kin and contact details;
- Current basic medical conditions (in case of emergency);
- Dietary requirements; and
- Records of conversations (behaviour, medical, mental health) if required.

From employees:-

- Name, address and contact details;
- Current basic medical conditions (in case of emergency); and
- Payroll and employment details;
- Educational qualifications and academic transcripts; and
- Records of conversations (behaviour, medical, mental health) if required.

6.2 Why we collect Personal Information

The College collects personal information for a variety of different purposes relating to its functions and activities including:-

- Enrolling and accommodating residents;
- Enhancing the resident experience and providing a range of services for the health and wellbeing of the residents; and
- Administering an employee's employment contract.

When collecting personal information by whichever means, the College will ensure that appropriate notices are given and consents obtained in accordance with the Australian Privacy Principles. Most information is collected directly from the individual. The College may also obtain some personal information from third party sources. In such cases the College will require a warranty from the third party that the information has been collected in accordance with Australian Privacy Principles, including notification that the information may be disclosed to organisations such as the College.

6.3 How we collect Personal Information

The personal information we require to deliver our services is usually collected directly from you:-

- using written forms;
- via the internet including websites and social media;
- via email;
- via telephone; and
- via face to face contact.

We may keep unsolicited personal information (personal information we receive that we have taken no active steps to collect) if the information is reasonably necessary for one or more of our functions or activities.

Our website uses cookies to provide a number of services to you and to us, such as data on user access on webpages. Cookies in use may identify individuals who log into our website. You can reject Cookies but doing so may limit your functionality and user experience within our site.

Note: Cookies provide information which is not classified as personal information

6.4 Disclosure of Personal Information

Personal information provided to the College will not be disclosed to other organisations or individuals without the provider's permission or when obliged to provide such information by lawful authority.

The College may disclose personal information for secondary purposes that are related to the primary collection purpose but only in situations where it is reasonable to expect such information to be disclosed.

The College will never sell, trade, lease or rent any personally identifiable information to other organisations.

6.5 Protection of Personal Information

Securing and protecting data is an issue that the College takes very seriously. We have implemented technology and security processes to protect the personal information that we collect and we take all reasonable steps to protect it. Our websites have electronic security systems in place, including the use of firewalls and data encryption. User identifiers and passwords are also used to control access to your personal information.

Specifically:-

- All authorised users are permitted to access the College IT Services, at a level commensurate with their position, role, delegated authority or student status;
- Access to all College IT Services will be removed when the relationship between Authorised Users and the College ceases;
- Authorised Users must not use their access to College IT Services to gain inappropriate personal, academic, financial or other advantage;
- Authorised Users must maintain the confidentiality of any Personal Information accessed via College IT Services; and
- Authorised users of College IT Services are not permitted to provide others with their Authentication Credential(s). It is the responsibility of Authorised Users to ensure that their Authentication Credentials are securely stores as they are responsible for all activity initiated from their account or with their Authentication Credential(s).

The College reserves the right to monitor, access, log and analyse the activities of Authorised users, and conduct reviews and audits as necessary.

The College reserves the right to block or filter any use that breaches this Policy or exceeds the College's acceptable level of risk.

The College may take any action deemed necessary to remedy immediate threats to the College IT Services or information and communications technology security including, without limitation, suspending an Authorised User's access, confiscation of College's owned electronic devices and/or disconnecting or disabling equipment with or without prior notice.[1]

6.6 Storage of Personal Information

The College's data is held in the Cloud which is stored outside of Australia, so potentially APP8 Cross-border disclosure of personal information applies. Note that our Cloud service provider has been certified by the Australian Signals Directorate through their ASD Certified Cloud Services program. Agreements with our Cloud service providers address compliance with Australian Privacy Laws and any amendment to those laws. We are confident that the providers will maintain administrative, technical, and physical safeguards to held protect the security, confidentiality and integrity of the College's data consistent with applicable requirements of Australian Privacy Laws.[2]

The College limits physical access to its offices. All personal information is maintained in controlled environments that are secured against unauthorised access.

6.7 Correcting, updating or deleting Personal Information

Every effort is made to ensure that personal information held is current, accurate and complete. In particular, residents can access, and are expected to update as necessary, their contact details and other personal information through the "StartRez" accommodation management system where Personal Information is stored.

Employees are able to correct information relating to their personal information by notifying their immediate supervisor of the need to update the information.

6.8 Accessing Personal Information

Any individual has the right to seek access to personal information held by contacting the College's Privacy Officer, either by writing or by email. The person seeking access will be asked to verify their identity before the information is released.

There are some exceptions to accessing personal information and the College will advise if the exception applies.

The College reserves its right to refuse access to employee records held by the College, where the personal information collected directly relates to the employment relationship between employer and employee. The release of this information will only be allowed at the College's discretion.

---

[1] The John Flynn College, *Information Technology Policy*, December 2022.
[2] Australian Government, Australian Signals Directorate, Cyber Security, https://www.cyber.gov.au/advice/cloud-computing-security

6.9 Complaints

Complaints concerning the collection, disclosure or handling of your Personal Information by the College should be addressed to the Privacy Officer. Any complaint should include the date, time and circumstances of the matter, how you believe your privacy has been breached and how you would like your complaint resolved.

The Privacy Officer will attempt to resolve the complaint within 5 business days but this timeframe may be extended if further information is required from the complainant and/or an involved third party. In managing the complaint, the Privacy Officer will follow principles of procedural fairness.

If the complaint is not resolved to your satisfaction you can refer it to the Office of the Australian Information Commissioner. Such complaints generally are resolved through conciliation.

7. THE AUSTRALIAN PRIVACY PRINCIPLES (APP)

(APP1) Openness and Transparency
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date Privacy Policy.

(APP2) Anonymity and Pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. The College falls within the exception to this APP as it would be impracticable for the organisation to deal with individuals anonymously or pseudonymously.

(APP3) Collection of Unsolicited Personal Information
Outlines when an APP entity can collect personal information that is solicited. It applies a higer standard to the collection of sensitive information. Personal information collected must be relevant for its function and activities. The College takes reasonable care, at the time of collecting personal information, or as soon as practical afterwards, to make an individual aware of why the information is collected, who it may be disclosed to, and how it can be accessed.

(APP4) Dealing with Unsolicited Personal Information
Outlines how an APP entity must deal with unsolicited personal information. The College will not collect information that it is not directed to collect and will destroy information that is received in error.

(APP5) Notification of the collection of Personal information
Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters. A privacy collection notice will be provided when collecting personal information addressing matters such as how and why the information is being collected.

(APP6) Use or Disclosure of Personal Information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds. The College will only use or disclose personal information for the **primary purpose** for which it was collected unless the **secondary purpose** is permitted under an exemptions.

(APP7) Direct Marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. The College will not release resident information for the purpose of direct marketing without the individual's consent.

(APP8) Cross Border Disclosure of Personal Information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas. The College will not release resident information overseas without the consent of the individual. The College would then ensure that the overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.

(APP9) Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual. The College will not adopt, use or disclose a government related identifier of an individual.

(APP10) Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure. The College will ensure that the personal information collected is accurate, up to date and complete.

(APP11) Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances. The College will ensure that all personal information is held in a secure environment with access to permitted staff only. When personal information is no longer required as per legislation the information is destroyed securely.

(APP12) Access to personal information
Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies. The College will provide personal information to the individual on request where applicable.

(APP13) Correction of personal information
Outlines an APP entity's obligation in relation to correcting the personal information it holds about individuals. The College will take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it's held, it is accurate, up to date, complete and not misleading.

8. DATA BREACHES

In the event of a suspected or actual data breach, the College will manage the process in accordance with the Data Breach and Response Procedure.

9. ASSOCIATED LEGISLATION AND INSTRUMENTS

Privacy Act 1988 (Cth)
Privacy Amendment (Notifiable Data Breaches) Act 2017
Data Breach and Response Procedure
Privacy Procedure

10. REVIEW

This policy will be reviewed annually.

11. ENDORSEMENT

Endorsed by the College Principal on 28/4/2020