EXCELSIA COLLEGE
Sydney-Australia

Document Name

PRIVACY POLICY

Document Number

PO-GEN-16

Document Status

Author	Chief Executive	January 2015
Approval	Management Committee	February 2015
Publication	Issue 4	July 2018
Review Date	Review of Issue 4	July 2022

Purpose and Scope

Excelsia College is committed to safeguarding personal information in accordance with the Privacy Act 1988 (**Act**). This policy describes the ways in which Excelsia College deals with personal information.

Excelsia College collects Personal Information and Personal Data from students and employees for the purposes of providing proper services. Any Personal Information and Personal Data collected from students and employees will be used by us in accordance with and as described in this Privacy Policy.

Definitions

Personal Information is defined in the Act as being information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information opinion is:

(a) true or not;
(b) recorded in a material form or not.

Personal Information includes, for example, names, addresses, telephone numbers, email addresses, dates of birth and passport numbers.

Sensitive information means personal information about you that is of a sensitive nature, including information about health, genetics, biometrics or disability; racial or ethnic origin; religious, political or philosophical beliefs; professional association or trade union memberships, sexuality; or criminal record. Special requirements apply to the collection and handling of sensitive information.

The Australian Privacy Principles

Excelsia College complies with the Australian Privacy Principles set out in the Privacy Act 1988 in respect of students' personal information. These principles are designed to protect your privacy. Therefore, Excelsia College employees will:

1. only collect personal information about you that is needed for us to offer you higher education services;
2. normally inform you if we are collecting information about you, why we need to do this, and who we would usually give that sort of information to;
3. do our best to ensure the information we collect from you is relevant, up to date and complete;
4. protect your information against any form of misuse, and prevent unauthorised use or disclosure;
5. maintain a statement of the types of personal information we hold and why we hold it, how long it is kept for, who can access it, and how people should go about getting access to it;
6. give you access to your personal information as held by Excelsia College, subject to restrictions in other government legislation;
7. update and amend our records of your personal information when you request such amendment;
8. take reasonable care to check that your information is accurate, up to date and complete, before using it;
9. only use your personal information for the purpose(s) for which it was collected;
10. not use your personal information for any purpose other than that for which it was collected, unless you consent, or the use is necessary to protect you against serious threat, or the use is required by law; and
11. in the case of 10 above, use or best endeavours to ensure that the recipient only use or disclose your information for the purpose for which it was given.

Collection and Use of Personal Information

Excelsia College collects information necessary to enable Excelsia College to:

- provide services to students and to people enquiring about study at Excelsia College
- process applications for admission
- communicate with students
- maintain appropriate academic and financial records
- perform other internal administrative functions
- maintain contact with alumni
- provide statistical and other information required by the government.

Personal information provided by you to Excelsia College will be used by us for the primary purpose for which you provided it and for other secondary purposes directly related to that primary purpose.

Disclosure of Personal Information

Excelsia College does not disclose personal information to third parties without the owner's consent, unless required or permitted by law.

Excelsia College may engage contractors located overseas for the limited purposes of storing students' personal information and ensuring that remains accessible upon demand on the terms of this Privacy Policy and only as part of the primary purpose for which it was provided (or for any secondary purposes directly related to that primary purpose). In that event, we will enter into a contract with the contractor requiring it to use the personal information only for the limited purpose of providing those services and otherwise abide by the terms of this Privacy Policy.

We may be required by law to disclose some personal information to Australian government organisations and to the Manager of the Tuition Protection Service.

Personal information may be disclosed for the prevention, detection or investigation of criminal or proscribed conduct, or in certain circumstances in the interest of public health or public safety.

We are required by law to inform the Australian Department of Immigration and Border Protection if an overseas student visa holder:

- changes the course of study for which s/he is enrolled
- changes the duration of his/her course of study
- breaches a student visa condition relating to attendance or satisfactory academic performance.

It may sometimes be necessary for Excelsia College to provide personal information to others with whom it conducts business, e.g. insurers, companies developing and providing educational software systems.

Lessen or prevent a serious threat

This permitted general situation applies to a serious threat to the life, health or safety of any individual, or to public health or safety. The permitted general situation would not apply after the threat has passed. A ‘serious’ threat is one that poses a significant danger to an individual or individuals. The likelihood of a threat occurring as well as the consequences if the threat materialises are both relevant. A threat that may have dire consequences but is highly unlikely to occur would not normally constitute a serious threat. On the other hand, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat, such as a threatened outbreak of infectious disease. This allows the College to take preventative action to stop a serious threat from escalating before it materialises.

The permitted general situation applies to a threat to life, health or safety. This can include a threat to a person's physical or mental health and safety. It could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. The permitted general situation would not ordinarily extend to a threat to an individual's finances or reputation.

The threat may be to an individual the College is dealing with or to another person. It may also be a threat of serious harm to an unspecified individual, such as a threat to inflict harm randomly.

A 'serious threat to public health or safety' relates to broader safety concerns affecting a number of people. Examples include:

- the potential spread of a communicable disease
- harm, or threatened harm, to a group of people due to a terrorist incident
- harm caused by an environmental disaster.

If time permits, attempts could be made to seek the consent from the relevant individuals for the collection, use or disclosure, before relying on this permitted general situation.

Any intended use of sensitive student information on the basis to lessen or prevent a serious threat should be made through a formal application.

Applications would include:

- substantive evidence provided to allow an assessment of the specific threat
- outline of the information to be released
    - information to be released
    - authorised recipients of the information (internal or external)
- intended use of the information.
- Approval

Use of Cookies

A "cookie" is a small text file which placed on your hard drive by some websites to store information about your visit to a website. A cookie only identifies your computer to a web server when you visit the site; they do not identify users.

We may use cookies to enhance the functionality of our website, to keep track of your visits to our website, and to enable us to provide personalised features on our website as part of our online services.

Web Beacons

A web beacon is an image that originates from a third party site to track visitor activities. We may use web beacons to track the visiting patterns of individuals accessing our website.

Data Breaches

What is a data breach?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of eligible data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- likely to result in serious harm to any of the individuals to whom the information relates
- the entity has been unable to prevent the likely risk of serious harm with remedial action
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

Consequences of a data breach

Data breaches can cause significant harm in multiple ways.
Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.
Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

The Notifiable Data Breaches scheme in Part IIIC of the Privacy Act 1988 (Cth) requires entities to notify affected individuals and the Commissioner of certain data breaches.

Below is the process map and guide in responding to data breaches.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Changes to Privacy Policy

Excelsia College reserves the right to modify and change this Privacy Policy at any time. Any changes to this policy will be published on our website.

Access to Your Personal Information

You have a right to access your personal information held by Excelsia College. You can also request amendment to that information if you believe that it is incorrect. To gain access to your personal information held by Excelsia College, complete the Student Request for Access to Own Personal Information form and send it to:

The Registrar, Excelsia College, 69-71 Waterloo Road, Macquarie Park NSW 2113.

Data Retention

We retain information you provide to us and which we collect about you, including Personal Information and Personal Data, for so long as we continue to provide services to you and for seven years after you have been with us.

Data Transfers

Sometimes, we transfer or disclose information to third parties including to persons and businesses outside Australia including in South East Asia. These transfers are made in order to assist us to provide you with the services we offer you. Where we transfer information to persons outside Australia we take reasonable steps to ensure that the recipients of such information do not breach the Australian Privacy Principles (and where appropriate the General Data Protection Regulation, GDPR) in relation to that information by entering into binding contractual arrangements with such third parties

Complaints about Privacy

If you have any complaints about our dealings with your Personal Information including any breaches by us of any Australian Privacy Principles or any questions regarding this Privacy Policy you are able to submit that complaint or query by contacting us at Excelsia.College@excelsia.edu.au.

Any complaints received by us will be referred to the Chief Executive for prompt investigation and a written response will be provided to you as soon as possible. Should you not be satisfied with the resolution of any complaints made you are able to seek further redress through the Office of the Australian Information Commissioner (see https://www.oaic.gov.au/for further information).

References and Related Documents

Avondale Privacy Policy (Higher Education)

University of New South Wales Privacy Policy

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme