APIC
ASIA PACIFIC
INTERNATIONAL COLLEGE

# DATA COLLECTION POLICY

| | |
|---|---|
| Document ID | Data Collection Policy |
| Related Documents | Records Management Policy<br>Privacy Policy<br>Health Information Collection Policy |
| Date | 16 December 2016 |
| Date of Next Review | 16 December 2018 |
| Authorised by | Director of Accreditation, Compliance and Quality Assurance |
| Approved by | Governing Board, 3 February 2017 |
| Version | 1.0 |
| Responsible Officer | ICT Manager |
| References and Legislation | The Privacy and Data Protection Act 2014<br>Education Services for Overseas Students Act<br>Education Services for Overseas Students Regulations 2001 (ESOS Act)<br>Tertiary Education Quality and Standards Agency Act 2011 (TESQA Act) |

## Contents

1. Purpose ....................2
2. Scope ....................2
3. Definitions ....................2
4. Privacy and Data Collection Law ....................2
5. Data Protection Risks ....................3
6. Responsibilities ....................3
7. General Staff Guidelines ....................4
8. Data Storage ....................4
9. Data Use ....................5
10. Data Accuracy ....................5
11. Subject Access Requests ....................6
12. Disclosing Data for Other Reasons ....................6
13. Providing information ....................6
14. Document Change Control ....................7

## 1. Purpose

APIC is required to gather and use certain information about individuals: customers, suppliers, business contacts, employees, students. and other people the College has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the College's data protection standards as well as legislative requirements.

This data protection policy ensures APIC:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

## 2. Scope

This policy applies to:

- The head office of APIC;
- All campuses of APIC;
- All staff and volunteers APIC; and
- All contractors, suppliers and other people working on behalf of APIC.

It applies to all data that the College holds relating to identifiable individuals, even if that information technically falls outside of the Privacy and Data Protection Act 2014. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers; and
- Any other information relating to individuals

## 3. Definitions

| **Item** | **Definition** |
|---|---|
| *Subject access requests* | Requests from individuals to see the data APIC holds about them. |

## 4. Privacy and Data Collection Law

The Privacy and Data Protection Act 2014 describes how organisations — including APIC — must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Privacy and Data Protection Act 2014 is underpinned by seven important principles, that data:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.

## 5. Data Protection Risks

This policy helps to protect APIC from some very real data security risks, including:

- Breaches of confidentiality: information being given out inappropriately.
- Failing to offer choice. All individuals should be free to choose how the College uses data relating to them.
- Reputational damage. The College could suffer if hackers successfully gained access to sensitive data.

## 6. Responsibilities

Everyone who works for or with APIC has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Governing Board** is ultimately responsible for ensuring that APIC meets its legal obligations.
- The **Executive Management Team** is responsible for:
  - Keeping the Governing Board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- The **ICT Manager** is responsible for:
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data APIC holds about them (also called ‘subject access requests’).
  - Checking and approving any contracts or agreements with third parties that may handle the College’s sensitive data;
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services, the College is considering using to store or process data. For instance, cloud computing services.

- The **Head of Marketing** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

## 7. General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees should request it from their line managers.
- APIC will provide **training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all **data secure**, by taking sensible precautions and following the guidelines below.
- S**trong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the College or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line-manager or ICT Manager if they are unsure about any aspect of data protection.

## 8. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the ICT Manager or ICT Team Leader. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the ECA's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

## 9. Data Use

Personal data is of no value to APIC unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The ICT Team Leader can explain how to send data to authorised external contacts.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

## 10. Data Accuracy

The law requires APIC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort APIC should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's de-tails when they call.
- APIC will make it easy for data subjects to update the information APIC holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Head of Sale's responsibility to ensure marketing databases are checked every six months.

## 11. Subject Access Requests

All individuals who are the subject of personal data held by APIC are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email. The ICT Team Leader can supply a standard request form, although individuals do not have to use this.

The ICT Team Leader will aim to provide the relevant data within 14 days.

The ICT Team Leader will always verify the identity of anyone making a subject access request before releasing any information.

## 12. Disclosing Data for Other Reasons

In certain circumstances, the Privacy and Data Protection Act 2014 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, APIC will disclose requested data. However, the ICT Manager will ensure the request is legitimate, seeking assistance from the Governing Board and from the College's legal advisers where necessary.

## 13. Disposal of Data

APIC will only dispose of data and records in accordance with the requirements of the state and federal government legislative instruments, including the ESOS Act, TEQSA Act and the Privacy and Data Protection Act. The destruction of data registered in the approved RMS will be managed centrally through the Director of Accreditation, Compliance and Quality Assurance, who will maintain a register of such.

Data must not be destroyed if it is, or may be, the subject of a subpoena, or other formal request for access or relate to any ongoing action such as an appeal, regardless of whether the minimum statutory retention period has expired.

## 14. Providing information

APIC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the College has a privacy policy, setting out how data relating to individuals is used by the company.  This is available on the College's website and in the APIC Policy Library.

## 15. Document Change Control

| Version | Change Description | Date | Author |
|---|---|---|---|
| 1.0 | Placed in new policy format | 16 December 2016 | Corinne Green |
| | | | |
| | | | |