CHS Data Collection Policy & Procedures

Document ID	**CHS Data Collection Policy & Procedures**
Category	Governance
Document Owner	Principal
Approved By	Governing Board
Authorised By	Governing Board

Version Control

Version	Summary of changes	Approval Date	Review Date
1.0	Document Established	Academic Board: 11 September 2018 Governing Board: 18 September 2018	20 September 2020

Table of Contents

1. Purpose

This policy describes how 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 CHS:

- 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 CHS;
- All campuses of CHS;
- All staff and volunteers CHS; and
- All contractors, suppliers and other people working on behalf of CHS.

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

Term	Definition
Subject access requests	Requests from individuals to see the data CHS holds about them.
Archive	Non-current records, for permanent retention.
Classification Scheme	Grouping records according to their functionality.
Disposal	The range of activities involved in retention, deletion or destruction of records.
Disposal Schedule	List of various records and the period of time the record must be retained. It may also indicate the time at which records should be transferred to secondary storage.
Destruction	Destroying a record, either the physical destruction or permanent deletion of a record.
Document	Information treated as a unit of information.
Record	Recorded information created or received by CHS that provides evidence of business activities and affairs, regardless of format.
Record Management System	Information system used to capture and provide access to records.

Term	Definition
Retention	The period of time a record should be retained by the institution before final disposal. It may also indicate when records should be transferred to secondary storage or Archived.

4. Policy Statements

Privacy and Data Protection Act 2014 describes how organisations — including CHS — must collect, handle and store personal information. These rules apply regardless of whether data are 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 2014 Act is underpinned by seven important principles, that data:

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

It is the College policy to ensure that all of data and records obtained are managed in accordance with the above principles and following the best practices supported by state-of-the art technologies and secure information systems. The CHS shall train the key staff to ensure that they are fully competent in managing the data and personal records obtained from students, staff and other stakeholders for the lawful purposes.

4.1 Data Protection Risks

This policy helps to protect CHS 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.

4.2 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.
- CHS 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.
- Strong 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.

5. Procedures

5.1 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 are 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 are 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 are 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.

5.2 Data Use

Personal data are of no value to CHS unless the business can make use of it. However, it is when personal data are 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.

5.3 Verification of Data

- Where staff enter data into external systems (such as HEIMS database, TEQSA Provider Portal) the staff member must have the accuracy of data entered verified by their direct supervisor and/or the Principal (where appropriate).
- This must be done prior to submission of data.

5.4 Data Accuracy

The law requires CHS to take reasonable steps to ensure data are kept accurate and up to date.

The more important it is that the personal data are accurate, the greater the effort CHS 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 are updated. For instance, by confirming a customer's de-tails when they call.
- CHS will make it easy for data subjects to update the information CHS holds about them. For instance, via the College 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.

5.5 Access to Records

Staff may have access to those records necessary to fulfil their duties.

- Certain records of a confidential nature may have restricted access for the period of time that they remain confidential.
- All requests by external agencies or individuals for access to records of a personal nature, other than their own record, must be referred to the Principal or the CHS Privacy Officer.

CHS records must remain on site with the exception of the following:

- Archived records may be stored off site with an approved service provider.
- Records are required to be made available to a court or for other legal purposes.
- Any other exceptional purpose with the approval of the Principal who may stipulate special conditions to be taken while the record is off site.

5.6 Access Requests

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

- Ask what information the College 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 College is meeting its data protection obligations.

If an individual contacts the College 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.

5.7 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, CHS 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.

5.8 Disposal of Data

5.8.1 CHS 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.

5.8.2 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.

6. Responsibilities

Everyone who works for or with CHS has some responsibility for ensuring data are 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 CHS meets its legal obligations.
- The Principal is responsible for ensuring data collection and management practices are compliant and the personnel assigned to manage these are trained to perform their duties in a compliant manner.
- The Principal 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 Support Officer** 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 CHS 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 **Marketing & Communications Officer** 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. Records

Records associated with this policy will be maintained according to the Records Management Policy and Record Retention and Disposal Schedule.

8. Related Documents

- CHS Records Management Policy
- CHS Privacy Policy
- CHS Health Information Collection Policy

9. Related legislation

- Higher Education Support Act 2003
- Tertiary Education Quality and Standards Agency (TEQSA) Act 2011
- TEQSA Higher Education Standards Framework (Threshold Standards) 2015
- Education Services for Overseas Students (ESOS) Act 2000 and National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code 2018)
- Australian Qualifications Framework (AQF)
- The Privacy and Data Protection Act 2014