



POLICY

**INFORMATION SECURITY AND
PROTECTION OF DATA COLLECTED
BY THE HIGHER EDUCATION
COMMISSION**

Version Control	
Policy Number	5-1
Status (draft version/approved)	Approved on 19 August 2020 at the 68 th Commission meeting
Policy owner	Senior Manager, Finance and Data Management Systems
Effective from	19 August 2020
Review date	18 August 2025

Key search words	Data Protection; Data Privacy; Data Protection Principles; Data Request; Data Access; Data Storage; Data Facilitation; Data Disclosure
-------------------------	--

Relevant legislation	Higher Education Act 2008 Higher Education Regulations 2009 Education Act 1966 Civil Service Act 1999
Related Commission documents: procedures/guidelines, etc.	Policy i-0-7 FHEC Roles and Responsibilities i-0-4-Guidelines: FHEC Communication Plan FHEC Internal HR policies, including Human Resources Policies, Guidelines and Procedures Manual 2016

Table of Contents	
Section	Page
1.0 Policy objective	2
2.0 Background	2
3.0 Definitions	3
4.0 Policy	4
13.0 Sign-off	9

1.0 POLICY OBJECTIVE

- 1.1. The policy ensures that the Higher Education Commission (Commission) is committed to protecting the privacy of data it collects and holds on Higher Education Institutions (HEI's), their students and graduates and institutional data from government organisations by addressing the following:
- i. Data privacy and safeguarding;
 - ii. Maintaining data integrity; and
 - iii. Ensuring the accountability of the Commission to its stakeholders.
- 1.2. This policy outlines how the Commission promotes and supports the principles of data protection. Particular reference is made to the purpose, collection, accuracy, consent, confidentiality, storage, access, retention, disclosure and data turnaround times in relation to data collected from HEI's, students, graduates and government agencies.

2.0 BACKGROUND

- 2.1 The Commission is vested with statutory powers to access and obtain information and documents from the HEI's as the Commission reasonably requires performing its mandated functions or exercise its powers as provided under section 7 of the Higher Education Act 2008 (the Act).
- 2.2 The Commission may require a higher education institution to provide such information as may be needed relating to any aspect of the institution's operation pursuant to section 50 of the Act.
- 2.3 As per mandatory legal requirement pursuant to *Regulation 33* of the Higher Education Regulations 2009; a registered institution must submit such information as the Commission may require for the purpose of monitoring compliance with the Act and maintaining its information management system.
- 2.4 The type of data regularly collected from HEIs, students, graduates and government agencies may include but is not limited to the following:
- a. Learner management records;

- b. Educational data, such as enrolment data, completion data, and graduate data;
- c. Students' demographic data and data on their destinations and outcomes;
- d. Financial data of HEIs;
- e. HEIs' staff information; and
- f. Unit cost per programme.

2.5 The Commission recognises the importance of data protection to safeguard the confidentiality and integrity of the different entities from which the Commission collects data from.

2.6 The adoption of data protection principles will govern the development of a standardised and systematic process concerning how Commission conducts the request, collection, storage, use, disclosure and protection of HEI, students and graduate data.

2.7 This policy, in conjunction with the Commission 's Policy Framework, is designed to address information security and data protection.

3.0 DEFINITIONS

Higher Education Institutions	An educational institution in or operating in Fiji that provides award-conferring post-secondary education or provides educational support services for students of other higher education institutions including overseas institutions, including but not limited to: <ul style="list-style-type: none"> a) Technical and vocational education and training centres; b) Information technology centres; c) Secretarial schools; d) Language schools; e) Hospitality training centres; f) Educational agencies; g) Caregiving training providers; h) Performing arts and sports academies; i) Religious, educational institutions; j) Colleges; and k) Universities.
Government agencies	Any agency that is part of the government, with whom the Commission from time to time may request data from. Examples of such agencies include the Fiji National Provident Fund (FNPF), the Fiji Revenue and Customs Services (FRCS), Tertiary Scholarship and Loans Board (TSLB) and the National Employment Centre (NEC).
Information	Any material in any form, including a record, report, correspondence, opinion, recommendation, press statement, circular, order, logbook, agreement, sample, model, data, or document such as: <ul style="list-style-type: none"> (a) A map, plan, drawing or photograph; (b) Any paper or other material on which there is a mark, figure, symbol or perforation that is capable of being interpreted;

	(c) Any article or material from which a sound, image or writing is capable of being reproduced with or without the aid of any other to or device; or (d) Any article on which information has been stored or recorded either mechanically or electronically.
Data Protection Principles	Provide the instruments to guide how Commission will conduct itself in the collection, storing, and use of data collected from HEIs. The Data Protection Principles are adopted from the European Union General Data Protection Regulation 2010 and contextualised to the Commission business operation.
General Data Protection Regulation 2010	A legal framework adopted by the European Union (EU) in April 2016 regarding data protection legislation. It applies to organisations or companies not established in the EU that offer goods and services to individuals in the EU or monitor their behaviour. It creates new rights for individuals in the digital environment and several new and detailed obligations for cooperation.
Data	Raw unanalysed, unorganised, unrelated, uninterrupted material which is used to derive information after analysis.
Central Depository Platform	A database infrastructure that is used to store varying data sets.

4.0 POLICY

4.1 This policy shall apply to activities related to the source, collection, storage and security, access, correction, accuracy, retention, use, and disclosure of data on HEIs, students, graduates and government entities.

4.2 All Commission personnel who are involved with the use of data on HEIs, students, Graduates and government entities must comply with this policy under the Commission's Code of Conduct, paragraphs 1 and 2.

Data protection principles

4.3 In the absence of any national laws on privacy in the country, the Commission adopts the Data Protection Principles (DPPs), which forms the instrument to standardised data protection.

4.4 The DPPs are adopted from the European Union Law, General Data Protection Regulation 2020 (GDPR). The DPPs are revised and contextualised into the Commission operation setting to address data protection of data on HEIs, students, and graduates.

4.5 The six (6) DPPs include:

- a. **Lawfulness, Fairness, and Transparency** – data collection practices should be conducted within the laws that represent the HEIs, students and graduates fairly; and that the Commission must disclose to HEIs, students and graduates the purposes for data collection and the reason(s) for the specified data collection.
- b. **Purpose Limitation** – the Commission should only collect data for a specific purpose, clearly state what the purpose is, and only collect data for as long as necessary to complete that purpose.
- c. **Data Minimisation** – the Commission undertakes not to collect data for which it has no clear and explicit purpose.
- d. **Accuracy** – the Commission will take reasonable steps to ensure data collected are accurate from the point of submission by HEIs, students and graduates and to use data in ways that give a fair and accurate representation.
- e. **Integrity and Confidentiality** – ensures appropriate security of the data on HEIs, students and graduates, including protection against unauthorised or unlawful processing, usage and accidental loss, destruction or damage, using appropriate technical or organisational measures undertakes to store and securely manage the data and to take all reasonable steps to guard against corruption, theft or unauthorised access.
- f. **Accountability** – ensures appropriate security of the data on HEIs, students and graduates, including protection against unauthorised or unlawful processing, usage and accidental loss, destruction or damage, using appropriate technical or organisational measures to store and securely manage the data and to take all reasonable steps to guard against corruption, theft and unauthorised access.

4.6 The DPPs shall govern the approach on the collection, storage and security, access, correction, accuracy, retention, use and disclosure of data on HEIs, students and graduates by the Commission.

Purpose

4.7 The Commission may require a higher education institution, student, graduate or a government agency to provide such information as may be needed relating to any aspect of the institution's operation.

4.8 In gathering the requisite information, the Commission may utilise such means as it considers necessary to acquire the information.

4.9 Under *Regulation 33*. Of Reg. 2009, a registered institution must provide such information as the Commission may require for the purpose of monitoring compliance

with the Act and maintaining its information management system.

- 4.10** Under *Regulations* 2009, Reg 42, pursuant to section 50 of the Act, the Commission may, by written notice require a person or institution to provide information and documents as the Commission reasonably requires to perform its functions or exercise its powers as provided for in these regulations.

Data collection and data accuracy

- 4.11** HEI data should be collected directly from an authorised individual representing the HEI or individual delegated by the HEI's authorised individual.
- 4.12** To protect HEIs, all data requests emanating from the Commission subgroups must be vetted internally by the Commission data committee made by representatives from the three main groups within the Commission, namely Operations and Quality Assurance, Corporate Services, and Finance and Data Management Systems, including the Senior Research Officer.
- 4.13** Student data may be collected directly from students or from the HEI where the student is or was enrolled or it may be accessed by the Commission from the Ministry of Education, Heritage and Arts' Fiji Education Management Information System (FEMIS).
- 4.14** Graduate data may be collected directly from graduates or from the HEIs where the graduate studied.
- 4.15** Where necessary, the Commission will collect data on HEIs, students and graduates from trusted public sources or other regulatory agencies.
- 4.16** The Commission takes all reasonable actions to ensure that the HEIs, students and graduate data collected, used and disclosed is accurate, complete and up to date. The Commission will work on the assumption that all data provided by the HEIs, students, graduates and government entities are accurate data, and that the Commission will be absolved of all responsibilities in case of incorrect data reporting, including potential consequences should incorrect data is supplied in part of HEIs, students, graduates and government entities.

Consent and confidentiality

- 4.17** When the Commission requests data from the HEIs, students, graduates or government entities, the Commission will ensure that the concerned HEI, student, graduate or government entity is made aware of the following concerns:
- a. the purpose of data collection;
 - b. their rights to access and correct the data being collected;
 - c. which party/parties will be privy to the collected data; and
 - d. how the Commission will store data.

- 4.18 The Commission will ensure confidentiality of all personal unit record details including names, addresses and contact details of students and graduates by controlling access to digital data by ensuring only individuals approved by the data vetting committee is granted access to the data.

Data storage, access, retention of HEI, student and graduate data

- 4.19 All data collected by the Commission must be stored securely in its central repository platform.
- 4.20 All data collected by the Commission must have a data backup file.
- 4.21 The HEIs, students or graduates has the right to access, correct or update their data if can be readily retrieved.
- 4.22 In case of a data breach, the Commission will take all necessary steps to secure its database, and at the same time provide an update to the HEI's, students, graduates and government entities of the extent of the data breach and steps taken by the Commission to mitigate against such data breach(s).
- 4.23 All data collected by the Commission will be stored indefinitely to carry out its legally mandated functions.
- 4.24 Decade-old data will be archived by the Commission's IT team in the Commission's central repository platform.

Data disclosure and data request turnover time

- 4.25 The Commission must provide HEIs, students, graduates and government entities a list of organisations and government entities that periodically requests data on HEIs, students and graduates from the Commission.
- 4.26 The Commission shall only disclose data requested from government agencies, HEIs, students and graduates if the Commission receives written authority from the HEI, student or graduate to disclose that information to a third party.
- 4.27 Aggregate data may be released given the approval from the Commission's Director.
- 4.28 The exception to compliance with clause 4.26 includes:
- a. The provider of the data was notified that other parties may be privy to the data when the data was requested.
 - b. That the data:

- i. Is to be used in a form in which the HEIs, student and graduate concerned are not identified;
- ii. Is to be used for statistical or research purposes and will not be published in any form that could reasonably be expected to identify the HEI, student or graduate concerned; or
- iii. The researcher signs an agreement to comply with the principles and requirements set out in 4.5, 4.6, 4.12, and 4.14 above.

4.29 If the Commission is legally obligated to disclose the data in accordance with existing Fiji laws, in which case, the Commission must identify the specific laws which the collection of the information is required and inform the HEI, student or graduate that the information has been disclosed in accordance with the law.

4.30 All data request must contain explicit descriptions of the following conditions:

- a. The purpose of the data request;
- b. List of the end-users of the data;
- c. How will the requestee use the data;
- d. The steps the requestee will take to avoid a misrepresentation of data; and
- e. How the data requestee will maintain the confidentiality of the data.

4.31 All requests for data from the Commission must require written approval from the Director of the Commission.

4.32 All data requests must be addressed to the Director of the Commission in writing.

4.33 For any data supplied by the Commission, the data requestee must supply the Commission with the final output(s) in which the data from the Commission was used.

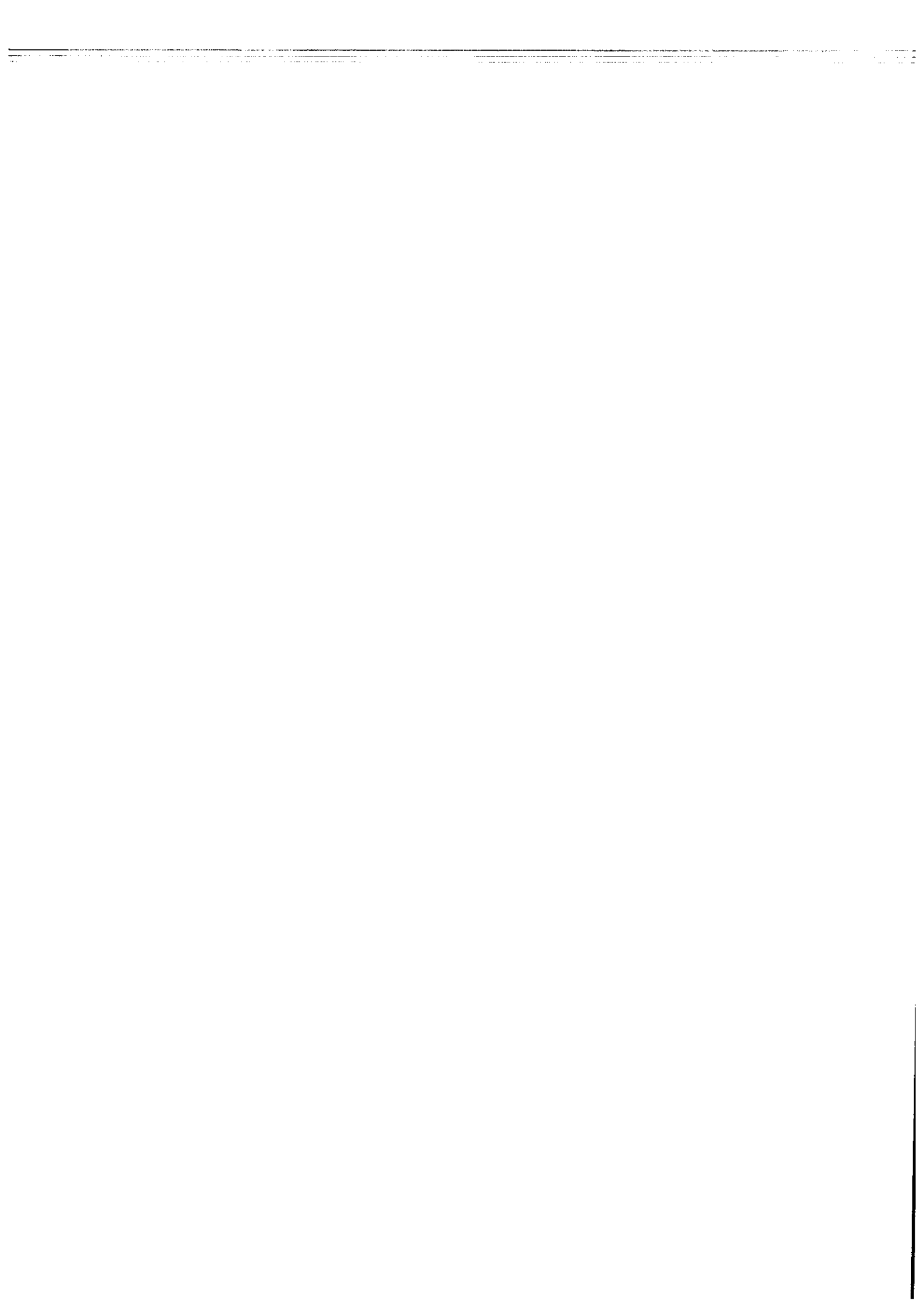
4.34 General data requests – such as enrolment and graduation data - from the Commission will be facilitated within a minimum of five working days. Complex data requests – such as data for survey samples - may take four to eight working weeks to be facilitated.

4.35 In case of a complaint from a stakeholder about data, then the Commission data vetting team will work with the senior management team and the senior research officer to address the complaints within two working weeks.

4.36 Data disclosure made to the Accountability and Transparency Commission will be exercised in accordance with the specified requirements in the Information Act 2018 when **this Act comes into force on a date or dates appointed by the Minister by notice in the Gazette and upon the establishment of the** Accountability and Transparency Commission.

Changes to this privacy statement

4.37 This policy will be reviewed every five years from the effective date; or



4.38 The Commission may amend this policy as our business requirements or the law changes.

5.0 APPROVAL BY THE CHAIRPERSON, HIGHER EDUCATION COMMISSION



Mr Julian Moti, QC
Chairperson
Higher Education Commission

Date 20.08.20