# Records and Data Management Procedure - Data

## Purpose

1. This Procedure outlines the process for the management of GHE's corporate, master and personal data to assure its quality, integrity and its proper management and protection.

## Scope

2. This Procedure applies to all GHE staff and its corporate, master and personal data in all formats, including:
   a) corporate data: facts as text, numbers, graphics, images, sound or video captured as an outcome of GHE's day-to-day operations. It can include, but is not restricted to staff data, student data, financial data, facilities data, curriculum data, etc.;
   b) master data: data about GHE entities that provide context for business transactions;
   c) personal data: data where a person's identity is apparent or can reasonably be ascertained.

## Definitions

3. Definitions for key terms are presented in the Glossary of Terms which may be accessed on the GHE website at https://www.globalhe.edu.au/policy

## Suite documents

4. This Procedure is linked to the following suite documents:
   a) Records and Data Management Policy;
   b) Records and Data Management Procedure – Records;
   c) Records and Data Management Procedure – Records: Schedule One - Records Retention and Disposal Authority.

## Procedure

### Data capture, processing, initial verification and quality

5. Data should only be collected where it serves a known and documented use, as per the provisions in the **Records and Data Management Policy**.
6. Effective data capture relies on knowledgeable staff, well-designed forms, databases and interfaces to ensure that all required data is collected in a form that meets organisational and reporting needs and ensures the production of high quality and targeted data.
7. Wherever possible data capture, processing and verification should be automated to maximise data quality.
8. Effective processes must be in place for the capture, maintenance and dissemination of high-quality data with all data required to confirm to the requirements of each field.
9. Data processing must be processed lawfully, fairly and in a transparent manner.
10. Initial verification of data must be undertaken by the Registrar when students are initially enrolled.

11. The Operations Director will appoint a Data Steward for each area. Data Stewards are responsible for:
    a) checks in relation to the accuracy and integrity of data produced in their area of responsibility;
    b) frequent review, update and reporting of new or revised data requirements;
    c) day-to-day management and oversight of quality of data produced in their area;
    d) overseeing and undertaking data quality audits and contributing to the resolution of identified issues in their area;
    e) being the key point of contact to assist with the effective implementation of this Procedure.
12. It is the responsibility of the Operations Director to undertake additional periodic quality checks to ensure adherence to business processes and high-quality data capture.
13. Staff members who identify data quality issues relating to accuracy, completeness, duplication and/or currency of data, or changes to business processes impacting on data collection and recording are required to report issues to the Operations Director. The Operations Director will convene an ad hoc Data Management Working Group to facilitate an appropriate organisational response to the issue raised.
14. Issues that may negatively impacting on ongoing compliance or contractual arrangements are to be reported to the Audit and Risk Committee by the Operations Director.

### Data storage, retention and disposal

15. Storage media used for the archiving of data must be appropriate for its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary or internal formats are involved.
16. Data storage systems are to be approved by the Operations Director and reported to the Audit and Risk Committee.
17. Corporate, master and personal data, whether physical or digital, must be stored in endorsed systems.
18. When permanently disposing of equipment containing storage media, all Confidential Data and licensed software must be irretrievably deleted before the equipment is moved off-site.
19. Data must be stored in an accessible form in accordance with the provision and minimum retention periods specified by the associated regulatory guidelines.
20. The timely destruction of data is essential for effective management. Electronic and physical data are destroyed by the authorised person after fulfilling the minimum retention period prescribed in the Records Retention and Disposal Authority attached as Schedule One to the Records and Data Management Procedure - Records.

### Data accessibility and security

21. Data sharing is encouraged, and data must be readily available to staff with a legitimate business need, except where the nature of the data requires restriction.
22. Access to data within GHE is restricted to authorised staff with the relevant business process need.
23. The extraction, manipulation and reporting of data internally should be for the purpose of informing GHE's teaching, management and governance requirements.
24. Where data is related to any aspect of the student experience from first contact through to alumni it must be used ethically, particularly in instances where GHE seeks to use such data to influence student behaviour either directly or indirectly. Any use outside that prescribed in the Offer Letter to students must be authorised by the Audit and Risk Committee.

25. Personal use of institutional data, including the derivation of data for personal research, in any format and at any location, is prohibited.
26. Where appropriate, before any data (other than publicly available data) is used or shared outside the GHE, verification from the Operations Director is required to ensure the quality, integrity and security of data will not be compromised.
27. Third parties who are provided with access to GHE data are required to sign a non-disclosure agreement.
28. Suitable controls are implemented for safeguarding sensitive data in GHE systems, including strong authentication for all access and encrypting data during transmission over public networks.
29. High security firewalls are used to control access to services or ports on servers that contain GHE data.

## Data reporting

### *Internal reporting*

30. GHE has data capture and reporting requirements that support internal processes such as:
    a) quality assurance of courses, academic progress monitoring and review, and management and monitoring of student and staff academic integrity, students with a disability, critical incidents, sexual assault and harassment incidents, and other management reports;
    b) strategic planning, performance monitoring and review; budgeting and financial reporting; asset registers; continuous improvement activities, and review of services and portfolio areas.
31. The processes and responsibilities for the analysis and reporting of data are outlined in each relevant policy (such as the **Academic Progress Policy**, **Student Academic Integrity and Misconduct Policy**, **Student Disability Policy**, **Quality Assurance Policy**) and in the terms of reference of governance committees.

### *External reporting*

32. GHE has an obligation to fulfil its data capture and reporting requirements to external agencies.
33. The Registrar is responsible for:
    a) the HEIMS Student and Staff Data Collection;
    b) all PRISMS reporting requirements.
34. The Academic Director is responsible for:
    a) reporting for Provider Information Requests (TEQSA);
    b) QILT reporting (Student Experience Survey, Course Experience Questionnaire, Graduate Outcomes Survey, Employer Satisfaction Survey).
35. Managers of other portfolio areas (for example, human resources and finance) are responsible for reporting to relevant agencies through GHE's governance structure.

## Overall data management

36. The Operations Director has overarching responsibility for ensuring that all data is captured and reported in accordance with external regulatory and contractual requirements.
37. The Operations Director is responsible for ensuring that data requirements are frequently reviewed and updated based on compliance requirement changes by regulatory bodies and changes to internal data and reporting processes.
38. The Board of Directors will be advised of any data requirement changes as they arise to ensure an organisational perspective of all data requirements is maintained.

39. The Operations Director maintains a register of endorsed systems and data stored in them.

### Metadata management

40. Metadata management is undertaken by information technology staff.

## Roles and responsibilities

41. The Board of Directors is responsible for oversight of this Procedure.
42. The Operations Director is responsible for:
    a) approving new and major changes to existing official data management systems;
    b) changes to the structure of official data management systems;
    c) changes to security levels within official data management systems;
    d) reporting to the Board of Directors regarding a) to c);
    e) nominating a Data Steward for each area;
    f) the maintenance of any records arising from this Procedure.
43. Managers of areas are responsible for:
    a) ensuring effective processes are in place for the capture, maintenance and dissemination of high-quality data by their area;
    b) ensuring all staff in their area are aware of their responsibilities and the key role they play in producing high quality data.
44. Data Stewards are responsible for:
    a) accuracy and integrity of data produced by their area;
    b) frequent review, update and reporting of new or revised data requirements;
    c) day-to-day management and oversight of quality of data produced by their area;
    d) overseeing and undertaking data quality audits and contributing to the resolution of identified issues in their area;
    e) being the key point of contact within each area to assist with the effective implementation of the Data and Records Management Policy and this Procedure.
45. Staff with the responsibility for data entry are responsible for the capture and maintenance of accurate data and ensuring data entered confirms to the requirements of each field.
46. Data users are responsible for:
    a) the accurate presentation and interpretation of data;
    b) releasing data only on the authority of the relevant manager.
47. The Manager, Quality and Compliance is responsible for:
    a) ensuring compliance with this Policy and related procedures;
    b) benchmarking GHE policy and standards with those adopted elsewhere in the higher education sector;
    c) the monitoring of information available from the review of records relating to the implementation of this Procedure.
48. It is the responsibility of all staff to understand their role in data capture, processing, verification to ensure the integrity and quality of all GHE corporate, master and personal data.

## Associated information

| | |
|---|---|
| **Related Internal Documents** | Records and Data Management Policy<br>Records and Data Management Procedure – Records<br>Records and Data Management Procedure – Records: Schedule One - Records Retention and Disposal Authority<br>Academic Progress Policy<br>Admissions Policy<br>Assessment Policy<br>Enrolment Policy<br>Financial Framework<br>Governance Framework<br>Human Resources Framework<br>Privacy Policy<br>Quality Assurance Policy<br>Risk Management Policy<br>Strategic Plan<br>Student Complaints, Grievances and Appeals Policy<br>Student Disability Policy<br>Student Diversity and Equity Policy<br>Student Sexual Assault and Sexual Harassment Policy<br>Teaching and Learning Plan<br>Glossary of Terms |
| **Related Legislation, Standards and Codes** | *Tertiary Education and Quality Standards Agency Act 2011*<br>*Higher Education Standards Framework (Threshold Standards) 2021*<br>TEQSA Guidance Notes: *Corporate Governance*, Version 2.4, *Academic Governance*, Version 2.3, *Monitoring and Analysis of Student Performance,* Beta Version 1.0<br>*Education Services for Overseas Students Act 2000*<br>*National Code of Practice for Providers of Education and Training to Overseas Students 2018*<br>*Freedom of Information Act 1991*<br>*Information Privacy Principles (IPP)*<br>*State Records Act 1998* (NSW)<br>*State Records Act 1997* (SA) |
| **Date Approved** | 1 May 2020 |
| **Date of Effect** | 1 May 2020 |
| **Date of Review** | June 2026 |
| **Approval Authority** | Board of Directors |
| **Policy Custodian** | Chief Executive Officer |
| **PinPoint DocID** | 2697 |

## Change history

| **Version Control** | | Version 1.3 |
|---|---|---|
| **Change Summary** | 23-Apr-20 | V1.0 Draft approved by Board of Directors (BoD) 1 May 2020 |
| | 23-July-20 | V1.1 Administrative updates |
| | 29-Nov-21 | V1.2 update for HESF 2021 |
| | 5-Oct-23 | V1.3 administrative updates following TEQSA |

Warning - Document uncontrolled when printed! The current version of this document is maintained on the GHE website at https://www.globalhe.edu.au/policy