



Data Protection Policy

Date of Approval: 20/ 10/2015

Date of Review: December 2016

Monitored By: College Management Committee

1.1. Introduction

Gaborone University College of Law and Professional Studies (GUC) is a registered and accredited tertiary education institution specializing in Law, Early Childhood Education and Business courses. It is a privately owned college. We offer high quality and valuable education which builds the trainees into committed and responsible leaders who have an entrepreneurial spirit to benefit the industry and society. We aim to contribute to the growth, global competitiveness and development of Botswana's economy through providing valuable human capital that the local and global market can rely on. GUC is a private institution registered by the Human Resources Development Council (HRDC) of Botswana. GUC offers programmes accredited by the Botswana Qualifications Authority (BQA)

1.2. Data protection Policy Statement.

Gaborone University College of Law and Professional Studies is committed to protecting the rights and freedoms of individuals. The requirements to which GUC staff and student who process personal data must adhere are set out in the college Data Protection Policy. The college explains the main purposes for which it processes the personal data of staff, students and persons who are neither staff nor students.

The primary purpose of current data protection policy is to protect the college and individuals against possible misuse of information by others. It is the policy of GUC to ensure that all members of the college and its staff are aware of the requirements of data protection policy under their individual responsibilities in this connection.

Gaborone University College of Law and Professional Studies abide by the data protection principles that require that personal data shall:

- be processed fairly and lawfully;
- be held only for specified purposes and not used or disclosed in any way incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate and kept up-to-date;
- not be kept for longer than necessary for the particular purpose;

- be processed in accordance with data subject's rights;
- be kept secure;
- Not be transferred outside to any other recipient unless the recipient ensures an adequate level of protection.

1.3. Responsibilities of the institution

To ensure that institutional information is safely kept, the college will

- Buy certified and approve software from accredited dealers
- Use certified companies to upgrade, change computer systems or process
- Back up all information in other electronic systems and hard copies
- Assign authority to relevant people to access file rooms and information lockers
- Maintain updated database for student, staff and other stakeholders
- Ensure information systems are protected by anti-virus software to minimise the possibility of data corruption
- Update information systems in line with the requirements of the government, external awarding boards and local regulatory authorities
- ensure that personal authentication is produced and recorded whenever a person request classified information relating to students ,staff or the college .

1.4. Responsibilities of staff

- All members of staff are responsible for ensuring that they adhere to the in the course of their employment.
- Staff is also responsible for ensuring that the personal data the college holds about them is accurate and up-to-date by informing the college of any changes or errors immediately.
- Heads of academic departments, colleges and support departments are responsible for ensuring that their respective departments comply with the college's data protection policy and procedures and shall actively promote compliance to their staff.

- Heads of departments and colleges are also responsible for ensuring that they nominate a departmental or college representative who will be responsible for data protection in their departments
- Refer any matter relating to release of data to higher authorities when they are in doubt.
- GUC systems are protected by 'individual user passwords which are individually accessible to staff responsible for processing data.
- GUC systems have the functionality to restrict access - users therefore only have access to data that enables them to carry out their job.
- Users who are given passwords should not exchange them whatsoever with colleges or friends in the workplace.

1.5. Responsibilities of Students.

Students agree to abide by the University's current data protection policy each year when they enrol.

Students are required to:

- Abide by the college Data Protection Policy.
- Allow the college to process their personal data
- All students are responsible for ensuring that they adhere to this policy.
- They are responsible for ensuring that the personal data the college holds about them is accurate and up-to-date by informing the college of any changes or errors immediately.
- Students who process personal data in connection with their course of study or extra-curricular, social or other activities undertaken as a GUC student or acting as a representative of the student body within their college or department, are permitted to do so after getting permission from relevant authorities.

1.6. Transfer of Data to Third Parties.

Personal data must not be disclosed to any third party (including family members and the police) except in the following circumstances:

- The data subject has given consent. This is unambiguously achieved by gaining written consent.
- It is necessary to protect the vital interests of the data subject.
- It is necessary to prevent serious harm to a third party.
- It is required to safeguard national security.
- It is necessary for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty.
- It is necessary for the discharge of regulatory functions including securing the health, safety and welfare of persons at work.
- It is to be used for research purposes, subject to the requirements of the research policy
- It is available to the public anyway by law.
- It is necessary to establish, exercise or defend legal rights.
- It has been published.

1.8. Monitoring and Policy Review

- The management of the college will monitor the implementation and revision of this Policy. Authority is delegated to the Heads of Departments and line managers to monitor activities in relation to this policy.
- The college Information Technology manager shall be responsible for the monitoring of all electronic information systems.
- Information collected will be reported to the management, and will be used to inform future equality and diversity work across the institution.
- The policy shall be reviewed in the event of changes in the information systems used by the college and changes in the operations strategy of the institution.
- This policy shall be reviewed in the event of a change to relevant legislation, and in any event on annual basis.