



DATA PRIVACY NEWSLETTER



“Privacy in Practice: Data Protection for Jamaica’s Colleges; what it means for the Council of Community Colleges of Jamaica (CCCJ)”.

In an era where data is as valuable as currency, protecting personal information is not just a legal requirement it’s a moral and institutional responsibility. With the enactment of Jamaica’s Data Protection Act (2020), all educational institutions, including community colleges and quality assurance bodies like CCCJ, must now align their data practices with national standards.

The Data Protection Act, 2020 (DPA 2020) governs the collection, processing, storage, and sharing of personal data. It came into full effect on December 1, 2023, after several years of transition.

The Act aligns with international standards such as the European Union’s General Data Protection Regulations (GDPR) and the United Kingdom’s Data Protection Act 2018 and applies to all entities (public and private) that handle personal data in Jamaica.

For the Council of Community Colleges of Jamaica (CCCJ), which plays a pivotal role in quality assurance and oversight for community colleges, the Act introduces significant responsibilities. CCCJ is considered a **third-party data controller**, meaning it processes personal data on behalf of the colleges it oversees.

WHAT IS THE DATA PROTECTION ACT?

The **Data Protection Act, 2020** is Jamaica’s first comprehensive law governing the collection, processing, storage, and sharing of personal data. It aims to protect the privacy rights of individuals and ensure that organizations handle data responsibly.

WHO IS A THIRD-PARTY DATA CONTROLLER?

A **data controller** is any entity that determines the purposes and means of processing personal data. While the CCCJ does not directly collect student’s data for academic delivery, processes such data during **enrolment, registration and evaluations**. This makes CCCJ a **third-party data controller**, acting on behalf of the colleges it oversees.

Understanding the Data Protection Act (2020) in Higher Education: key provisions and their application to CCCJ.

The CCCJ like all other higher education institutions is required to utilize the key Core Data Protection Principles to guide their operations.

1. CCCJ must adhere to the following principles when handling personal data:

- Lawfulness, Fairness, and Transparency – Data must be processed legally and fairly, with clear communication to data subjects.
- Purpose Limitation – Data must be collected for specific, legitimate purposes (e.g., certification, audits, staffing).
- Data Minimization – Only the data necessary for the task should be collected.
- Accuracy – Data must be kept accurate and up to date.
- Storage Limitation – Data should not be kept longer than necessary.
- Integrity and Confidentiality – Data must be protected against unauthorized access or loss.
- Accountability – CCCJ must demonstrate compliance with all principles.
- Cross border transfer – Organizations should ensure that any data in their custody that is processed/stored outside of Jamaica should be processed in countries with adequate data protection laws.

2. CCCJ must ensure that individuals (staff) whose data it processes can exercise their rights, including:

- Right to Access – Request a copy of their personal data.
- Right to Rectification – Correct inaccurate or incomplete data.
- Right to Erasure – Request deletion of data under certain conditions.
- Right to Object – Object to data processing, especially for non-essential purposes.
- Right to Data Portability – Transfer their data to another institution in a structured format.

3. CCCJ as a Data Controller and Data Processor

Although CCCJ does not directly enroll students, it processes student and staff data during:

- Institutional audits
- Awarding of certificates
- Recruitment and training of staff
- Data reporting to the Ministry of Education, Skills, Youth and Information

This makes CCCJ a third-party data controller, responsible for ensuring that all data it receives from colleges is handled in compliance with the DPA 2020.

4. Obligations of CCCJ

As a data controller and Data Processor, CCCJ must:

- Obtain data lawfully from colleges with proper consent or legal basis.
- Use data only for quality assurance purposes.
- Implement technical and organizational safeguards (e.g., encryption, access controls).
- Maintain a data processing register documenting all data activities.
- Ensure contracts with processors (e.g., IT vendors) include indemnity clauses.



CONCLUSION

As a steward of educational quality, CCCJ must also be a steward of **data privacy**. By aligning with the Data Protection Act, CCCJ not only complies with the law but also reinforces its commitment to ethical and responsible governance in Jamaica's higher education sector.

REFERENCES:

- Data Protection in Action: Empowering CCCJ to Lead with Privacy
- Data Protection Act 2020 Overview
- The UWI Data Protection Office