

Financial Policies

NAME OF POLICY	Financial Policy No. 4 – Bank Account and Credit Card Privacy Policy		
APPLICABLE SECTIONS OF THE ACT, BY-LAWS AND REGULATIONS and/or PURPOSE	Ensuring Effective Stewardship of CPATA Assets Protection of privacy		
RESPONSIBILITY	CEO and all CPATA employees and consultants		
APPROVED BY	EFFECTIVE	REVIEWED	REVISED
Chief Executive Officer	2021-12-01	2025-07-15	2025-09-30

1. Rationale

The College must protect the privacy of all parties including the information on Bank Accounts and Credit Card details that the College receives for the purpose of processing licence and other fees from licensees and firms. In addition, the College receives bank account information for the purpose of making payments to Board and Committee members, suppliers and employees.

2. Policy

As explained in the College's Governance Policies, Appendix K – Privacy Policy, the College's Policy Statement on Privacy is:

"Personal information in the College's custody or under its control is only created, collected, retained, used, disclosed and disposed of in a manner that respects and complies with the Privacy Act and its Regulations and aligns with TBS privacy policies and directives. The College upholds the privacy rights of individuals whose personal information is controlled by the College, in accordance with these requirements."

3. Protocol

1. Credit Card and Banking information for processing payments:

Currently, the College receives an application or payment form and/or email from an individual that includes credit card and/or bank account information for the purpose of processing payment in the financial systems.

The goal is to remove this requirement for emails and forms for payments of fees and move all payments into the College's Licence database system once the registration and applicable modules are fully developed.

When this credit card and/or bank account (payment information) is received and the payment is processed, the College must ensure as soon as possible that:

- the payment information must be redacted from the application or payment form if the document is going to be saved in College's electronic files.
- the email that was received will either be permanently deleted, or the attachment removed from the email if the email will be saved. This must be done by all College employees and consultants.

CPATA reimburses only those reasonable expenses necessarily incurred while travelling on CPATA business. These expenses do not constitute income or other compensation that would open the way for personal gain. Any deviations from the policy must be approved by the CEO and/or Chair of the Board in writing before reimbursement will be made.

2. Banking information for payments to suppliers and employees:

The College currently makes all payments to suppliers electronically and requires bank account information from suppliers in order to make the payment. This information is normally contained on the supplier invoice and/or provided as a separate form. This information must be kept on file by the College for current and future payments.

The College also requires bank account information for employees and Board and Committee members for payroll purposes. This information is received as part of the new hire onboarding process. This bank account information must be safeguarded and kept private. This includes being kept on the College's server within a firewall. This includes email that is protected by a firewall.

3. Refund Processing

If the College must provide a payment refund to a licensee or other individual, the refund shall be paid back using the same method and to the same account as the initial transaction. Credit Card payments are to be processed by the CFO or Administrative Coordinator in the licensee management or Moneris systems. E-transfers, wire payments and direct deposits will be paid through RBC Express via an Electronic Funds transfer. CPATA will not send email money transfers.

4. Privacy Breach

If there is a breach of the individual's bank account information, the College's Privacy Officer must be notified along with the individual whose information may have been breached. Appropriate steps will be taken in accordance with the College's Governance Policies, Appendix K – Privacy Policy.