The Cyberfront Institute – Policy Framework

(Trinidad & Tobago)

1. Introduction

This Policy establishes the governance, operational, financial, and ethical standards of **The Cyberfront Institute**, a registered non-profit organisation in Trinidad & Tobago. It ensures compliance with national legislation, protects beneficiaries, guarantees transparency, and strengthens accountability to donors, partners, and the wider community.

2. Vision & Mission

- **Vision:** To empower communities in Trinidad & Tobago through education, technology, and social development initiatives, creating opportunities for growth and resilience.
- **Mission:** To deliver accessible, innovative, and impactful programs that support children, youth, parents, and underserved groups, fostering digital literacy, financial inclusion, and sustainable community development.

3. Core Values

- Integrity
- Accountability
- Transparency
- Inclusiveness
- Innovation
- Community Empowerment
- Sustainability

4. Legal & Regulatory Compliance

4.1 Registration & Oversight

- The Cyberfront Institute is registered in accordance with the **Non-Profit Organisations Act, 2019 (NPO Act)**.
- All governance documents (constitution, bylaws, list of controllers, audited accounts) shall be maintained and updated as required.

- If annual gross income exceeds **TT$500,000**, the Institute shall comply with **Financial Intelligence Unit (FIU)** supervision and reporting obligations under AML/CFT regulations.

4.2 Charitable Status & Tax Exemptions

- Applications for charitable status shall be made through the **Ministry of Finance** under **Section 6(1)(g) of the Corporation Tax Act, Chap. 75:02**.
- The Institute shall maintain eligibility by providing audited financial statements, activity reports, and evidence of public benefit.

4.3 Other Laws

The Cyberfront Institute shall operate in compliance with:

- **Consumer Protection and Fair Trading Act, 2020**
- **Children's Act, Chap. 46:01**
- **Domestic Violence Act**
- **Occupational Safety and Health Act**
- **Data Protection Act**
- All other relevant national legislation.

5. Governance & Leadership

- The Cyberfront Institute shall be governed by a **Board of Directors** responsible for strategic oversight, fiduciary responsibility, and policy approval.
- An **Executive Director** and management team shall oversee daily operations.
- Clear separation of governance (Board) and management (staff/volunteers) shall be maintained.
- All Board members must declare conflicts of interest and act in the best interest of the Institute.
- Policies shall be reviewed every **two (2) to three (3) years** or sooner if required.

6. Membership & Stakeholder Participation

- Membership shall be open to individuals and organisations aligned with the Institute's mission.
- Rights include participation in general meetings and decision-making where applicable.
- Responsibilities include adherence to policies, ethical conduct, and support of the Institute's goals.

- Stakeholders — including beneficiaries, parents, and community partners — will be regularly consulted through forums, surveys, and open dialogues.

7. Policy Towards Customers, Beneficiaries & Underserved Persons

7.1 Equity & Inclusion

- The Cyberfront Institute is committed to serving all persons **without discrimination**.
- Priority shall be given to underserved groups such as children from low-income families, rural communities, single-parent households, persons with disabilities, and at-risk youth.

7.2 Accessibility & Empowerment

- Programs will remain **affordable and accessible**, leveraging sponsorships and donor support to reduce barriers.
- Beneficiaries will be empowered to grow beyond recipients, becoming active participants and community leaders.

7.3 Customer Care & Consumer Rights

- All beneficiaries are entitled to:
    - Respectful, fair, and dignified treatment.
    - **Clear, upfront information** on services, costs, and eligibility.
    - **Confidential handling** of personal data.
- A **Customer Charter** shall be published in simple language for community use.

7.4 Financial Accountability & Consumer Protection

- The Institute shall operate in accordance with the **Consumer Protection and Fair Trading Act, 2020**.
- **Banking systems** (bank transfers, direct deposits, cheques, POS transactions) shall be the **primary payment method**.
- **Cash payments** are strongly discouraged; if unavoidable, they must be receipted and deposited within **two (2) working days**.
- All transactions must be traceable, receipted, and auditable.
- Refunds, where applicable, shall be processed through secure banking channels.

7.5 Feedback & Complaints

- Beneficiaries may provide feedback or lodge complaints through:
    - Suggestion boxes
    - Online forms
    - Telephone hotline

    - Community forums
- All complaints shall be handled fairly, confidentially, and promptly, with whistleblower protection.

7.6 Safeguarding & Protection

- Zero tolerance for exploitation, neglect, or abuse.
- Staff and volunteers working with children or vulnerable groups shall undergo background checks.
- All safeguarding practices shall comply with national protective laws.

8. Human Resources & Conduct

- Recruitment shall be transparent and non-discriminatory.
- All staff and volunteers must sign a **Code of Conduct** covering ethics, safeguarding, confidentiality, and professionalism.
- Training and development opportunities shall be provided.
- Grievances shall be handled fairly, with documented procedures.

9. Financial Management & Reporting

- Annual budgets must be prepared and approved by the Board.
- **Dual authorization** is required for major disbursements.
- Quarterly financial reports will be shared with the Board.
- Annual independent audits (ICATT-certified auditor) are mandatory.
- Summaries of financial statements shall be shared with stakeholders for transparency.

10. Programs, Projects & Community Development

- Programs must align with the **National Policy on Sustainable Community Development (2019-2024)**.
- Needs assessments and stakeholder consultations will guide program design.
- Monitoring and Evaluation (M&E) will ensure measurable outcomes and impact.
- Partnerships will be formalized through MOUs with clearly defined responsibilities.

11. Data Protection & Confidentiality

- All personal and sensitive data will be handled in compliance with the **Data Protection Act**.

- Access to records shall be restricted and controlled.
- Beneficiaries may request access to their personal data held by the Institute.

12. Risk Management & Internal Controls

- The Cyberfront Institute shall maintain a **risk register** covering financial, legal, operational, and reputational risks.
- Disaster preparedness and crisis management plans shall be developed.
- Insurance will be obtained where necessary to protect assets and staff.

13. Transparency & Accountability

- Annual reports will be prepared and made available to regulators, donors, and the public.
- Key information (program impact, financial statements) will be accessible to stakeholders.
- Procurement and contracting will be **transparent, competitive, and documented**.

14. Amendments

- This Policy may be amended by a **two-thirds majority vote of the Board of Directors**, after consultation with members and stakeholders, in compliance with the NPO Act and the Institute's Constitution.

15. Effective Date

This Policy shall take effect on **05th August, 2025** and remain valid until reviewed or replaced.