DATA PRIVACY POLICY
City College of Cagayan de Oro
Version 1.0 • Effective 2025

PART I
PRELIMINARY PROVISION

A. Declaration of Policy

The City College of Cagayan de Oro (CCCDO), through its Technology Innovation and Data Management Center (TIDMAC), recognizes and upholds the fundamental right to privacy and the corresponding responsibility to protect personal data entrusted to the institution by its students, parents, guardians, applicants, alumni, employees, and other stakeholders. The College acknowledges that the responsible processing of personal information is essential in the fulfillment of its mandate as a public higher education institution committed to providing quality, accessible, relevant, and inclusive education.

In the exercise of its academic, administrative, research, extension, and public service functions, the College necessarily collects, records, organizes, stores, uses, shares, retains, and disposes of personal data. Recognizing the importance of protecting the rights and freedoms of data subjects, the College shall ensure that all personal data processing activities are conducted in a lawful, fair, transparent, and secure manner.

Consistent with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012; its implementing rules and regulations; issuances of the National Privacy Commission; applicable policies of the Commission on Higher Education; and relevant policies and regulations of the City Government of Cagayan de Oro, the College shall observe the principles of transparency, legitimate purpose, and proportionality in all personal data processing activities. The College shall likewise adopt reasonable and appropriate organizational, physical, and technical safeguards to protect personal data against unauthorized access, disclosure, alteration, misuse, destruction, or loss.

As the college's lead office for technology innovation, information management, data governance, digital transformation, and information security, the Technology Innovation and Data Management Center (TIDMAC) shall support the implementation of this policy by promoting privacy awareness, strengthening information security practices, supporting institutional compliance initiatives, and fostering a culture of accountability and responsible data stewardship throughout the college community.

The College further recognizes that privacy protection is a shared responsibility among administrators, faculty members, employees, students, service providers, and other stakeholders. Accordingly, all persons involved in the processing of personal data shall be expected to uphold the highest standards of confidentiality, integrity, professionalism, and accountability in accordance with applicable laws, regulations, and institutional policies.

Through this Privacy Policy, the City College of Cagayan de Oro reaffirms its commitment to safeguarding personal data, protecting the rights of data subjects, promoting responsible information management, and strengthening public trust in the institution as it pursues excellence in higher education, innovation, and public service.

B. Scope

This Privacy Policy applies to all personal data processed by the City College of Cagayan de Oro (CCCDO) concerning its students, applicants, parents, guardians, alumni, scholarship beneficiaries, research participants, and other individuals whose personal information is collected, maintained, or processed by the College in the performance of its educational, administrative, research, extension, and public service functions.

This Policy governs the collection, recording, organization, storage, updating, retrieval, consultation, use, disclosure, sharing, transfer, retention, archiving, disposal, and destruction of personal data processed through both manual and automated means. It covers all forms of personal data maintained by the college, whether contained in physical records, electronic databases, information systems, cloud-based platforms, learning management systems, websites, mobile applications, surveillance systems, communication platforms, and other technologies utilized by the institution.

The provisions of this Policy shall apply to all officials, faculty members, administrative personnel, contractual employees, student assistants, consultants, researchers, service providers, and third-party partners who process personal data on behalf of the College. Such persons shall be required to comply with the Data Privacy Act of 2012, its implementing rules and regulations, National Privacy Commission issuances, applicable Commission on Higher Education policies, and the privacy and information security policies of the college.

As the college's lead office for technology innovation, data governance, information management, digital transformation, and information security, the Technology Innovation and Data Management Center (TIDMAC) shall assist in the implementation, monitoring, and continuous improvement of privacy and data protection measures under this policy. TIDMAC shall support academic and administrative offices in ensuring that personal data are processed securely, responsibly, and in accordance with applicable laws and institutional standards.

This Policy shall apply to all activities involving personal data undertaken within college premises, through official college systems and platforms, during off-campus

activities authorized by the college, and in other circumstances where personal data is processed under the authority or responsibility of the City College of Cagayan de Oro.

C. Legal Bases

This Privacy Policy is established pursuant to the constitutional and statutory mandate to respect, protect, and uphold the right to privacy and the protection of personal data. The City College of Cagayan de Oro recognizes that the responsible processing of personal information is essential to the effective delivery of higher education services, institutional governance, and public accountability. Accordingly, this policy is guided by applicable national laws, regulatory issuances, higher education policies, and local government regulations governing data privacy, records management, information security, and educational administration.

This Policy is primarily anchored on Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, and its Implementing Rules and Regulations (IRR), which establish the framework for the protection of personal data and safeguard the rights of data subjects while ensuring the free flow of information necessary for innovation, growth, and public service.

In the implementation of this policy, the college shall likewise observe and comply with relevant issuances of the National Privacy Commission (NPC), including but not limited to:

a. NPC Circular No. 16-01, *Security of Personal Data in Government Agencies*;

b. NPC Circular No. 16-03, *Personal Data Breach Management*;

c. NPC Circular No. 17-01, *Registration of Data Processing Systems and Notification Regarding Automated Decision-Making*;

d. NPC Circular No. 2022-01, *Guidelines on Administrative Fines*; and

e. Other applicable NPC Circulars, Advisory Opinions, Memorandum Circulars, Commission Issuances, and related regulatory issuances that may be promulgated or amended from time to time.

As a higher education institution, the College shall likewise be guided by Republic Act No. 7722, otherwise known as the Higher Education Act of 1994, and by policies, standards, and guidelines issued by the Commission on Higher Education (CHED). These include, among others, CHED Memorandum Order No. 9, Series of 2013, or the

Enhanced Policies and Guidelines on Student Affairs and Services, quality assurance policies, accreditation standards, records management requirements, Higher Education Management Information System (HEMIS) reporting requirements, and other relevant CHED issuances affecting the processing of student information and institutional records.

The College shall further comply with Republic Act No. 10931, otherwise known as the Universal Access to Quality Tertiary Education Act, insofar as personal data processing is necessary for the administration of scholarships, grants, financial assistance programs, and related educational benefits. It shall likewise observe Batas Pambansa Blg. 232, otherwise known as the Education Act of 1982, in relation to the rights and responsibilities of educational institutions, students, parents, and other stakeholders.

To ensure proper records governance and preservation of institutional records, this policy is also guided by Republic Act No. 9470, otherwise known as the National Archives of the Philippines Act of 2007, including applicable records retention, archiving, and disposal requirements.

As a local higher education institution established and supported by the city government of Cagayan de Oro, the college shall likewise observe applicable city ordinances, executive issuances, data privacy notices, information security policies, administrative regulations, and other local government measures relating to privacy protection, information management, cybersecurity, digital governance, and public accountability.

The implementation of this policy shall also be informed by evolving best practices in privacy governance, information security, digital transformation, records management, and higher education administration. The College, through its Technology Innovation and Data Management Center (TIDMAC) and other responsible offices, shall continuously review and update its policies and practices to ensure compliance with applicable laws and responsiveness to emerging privacy and security risks.

D. Definition of Terms

For purposes of this Policy, the following definitions shall apply:

1. **Personal Data** refers to any information, whether recorded in material form or not, from which the identity of an individual is apparent or can reasonably and directly be ascertained by the entity holding the information. It includes personal information, sensitive personal information, and privileged information relating to an identified or identifiable natural person.

2. **Sensitive Personal Information** refers to personal data that is more sensitive in nature and requires a higher level of protection under applicable privacy laws. This includes information relating to an individual's race, ethnic origin, marital status, age, color, religious, philosophical, or political affiliations; health, education, genetic, or biometric information; sexual orientation or sexual life; information regarding any criminal, administrative, or disciplinary proceedings; government-issued identifiers; and other information classified by law as sensitive.
3. **Data Subject** refers to any natural person whose personal data is collected, processed, stored, shared, or otherwise handled by the City College of Cagayan de Oro. Data subjects include, but are not limited to, students, faculty members, administrative personnel, applicants, alumni, contractors, service providers, visitors, and other stakeholders whose information is processed by the institution.
4. **Personal Information Controller (PIC)** refers to the natural or juridical person, public authority, agency, or other body that controls the collection, holding, processing, or use of personal data. For purposes of this policy, the City College of Cagayan de Oro (CCCDO), through the Technology, Information, Data Management, and Communications (TIDMAC) Office and authorized institutional offices, acts as the personal information controller and is responsible for ensuring compliance with applicable data privacy laws and regulations.
5. **Personal Information Processor (PIP)** refers to any natural or juridical person, public authority, agency, or other body to whom a Personal Information Controller may outsource or delegate the processing of personal data. A Personal Information Processor acts only upon the instructions of the Personal Information Controller and is required to implement appropriate security and privacy safeguards in accordance with contractual agreements and applicable laws.
6. **Data Privacy Officer (DPO)** refers to the duly designated officer responsible for overseeing and ensuring the institution’s compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), issuances of the National Privacy Commission (NPC), and this policy. The DPO serves as the focal point for privacy-related concerns, complaints, breach management, awareness activities, and coordination with regulatory authorities.
7. **Processing** refers to any operation or set of operations performed upon personal data, whether by automated means or otherwise. This includes, but is not limited to, the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, consolidation, blocking, erasure, destruction, disclosure, transfer, sharing, dissemination, or any other handling of personal information.
8. **Data Breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, acquisition of, or use of personal data. Data breaches may result from cyberattacks, human error, system failures, unauthorized access, theft, or other incidents that

compromise the confidentiality, integrity, or availability of personal information.

9. **Consent** refers to any freely given, specific, informed, and unambiguous indication of the will of a data subject whereby he or she agrees to the collection and processing of personal data relating to him or her. Consent may be expressed in writing, electronically, or through any lawful means recognized under applicable regulations.
10. **Information and Communications Technology (ICT) Resources** refers to all hardware, software, networks, databases, cloud services, communication systems, applications, digital platforms, and electronic devices owned, managed, administered, or utilized by the college for academic, administrative, research, and operational purposes.
11. **Confidentiality** refers to the principle that personal data shall be protected against unauthorized access, disclosure, or misuse and shall only be made available to authorized individuals with legitimate purposes and appropriate authority.
12. **Integrity** refers to the accuracy, completeness, consistency, and reliability of personal data throughout its lifecycle and the assurance that information is not improperly altered, modified, or destroyed.
13. **Availability** refers to the principle that authorized users shall have timely and reliable access to personal data and information systems whenever necessary for legitimate institutional purposes.
14. **Data Retention** refers to the period during which personal data is maintained, stored, and preserved by the institution in accordance with legal, regulatory, administrative, academic, and operational requirements before its secure disposal or destruction.
15. **Data Disposal or Destruction** refers to the process of permanently deleting, erasing, shredding, anonymizing, or otherwise rendering personal data unreadable, inaccessible, and irrecoverable once the retention period has expired or when the data is no longer necessary for legitimate purposes.

PART II
DATA COLLECTION AND PROTECTION OF PERSONAL DATA

A. Data Life Cycle

Personal data collected by the college undergoes a life cycle consisting of collection, storage, use, sharing, retention, and disposal. Throughout these stages, the College shall adopt appropriate safeguards and ensure that the principles of transparency, legitimate purpose, and proportionality are observed.

In accordance with the Data Privacy Act of 2012, CHED regulations, and applicable policies of the City Government of Cagayan de Oro.

1. Collection

The College collects personal data necessary for the performance of its educational, administrative, research, extension, and public service functions.

Personal data collected may include, but is not limited to:

- Personal and demographic information, including name, sex, age, civil status, citizenship, nationality, date and place of birth, and photograph;
- Contact information, including residential address, email address, telephone number, mobile number, and emergency contact details;
- Academic information, including educational background, admission records, enrollment information, grades, academic standing, and disciplinary records;
- Financial information relating to scholarships, grants, educational assistance, and tuition subsidies; and
- Health and wellness information necessary for the provision of student support services and emergency response.

2. Recording

Collected personal data may be documented, encoded, or entered into authorized records and information systems maintained by the college.

Recorded information may include, but is not limited to:

- Admission and enrollment records;
- Student information system entries;
- Academic and scholastic records;
- Scholarship and financial assistance records;
- Guidance, counseling, and health service records; and

- Records of official transactions involving students, parents, and guardians.

3. Organization

Personal data may be classified, indexed, categorized, and arranged to facilitate efficient retrieval, management, and protection of records.

Organized records may include the following, but are not limited to:

- Student records arranged by academic program, year level, or student number;
- Academic records classified by semester or academic year;
- Scholarship and financial assistance records categorized by program or funding source;
- Personnel and administrative records maintained by authorized offices; and
- Electronic records organized within institutional databases and information systems.

4. Storage

Personal data shall be maintained in secure physical and electronic repositories protected by appropriate safeguards.

Storage facilities and repositories may include, but are not limited to:

- Filing cabinets and records storage rooms;
- Institutional databases;
- Learning management systems;
- Authorized cloud-based storage solutions;
- Backup servers and storage media; and
- Other information systems approved by the College.

5. Use

Personal data may be used only for lawful, legitimate, and declared purposes consistent with the functions of the college.

Such use may include, but is not limited to:

- Processing admissions and enrollment;
- Evaluating academic performance and graduation requirements;
- Administering scholarships, grants, and financial assistance programs;
- Providing student affairs and support services;
- Conducting institutional research and assessment activities; and

- Preparing reports required by law or regulatory agencies.

6. Disclosure and Sharing

Personal data may be disclosed or shared when authorized by law, required by regulatory obligations, necessary for institutional functions, or with the consent of the data subject, as applicable.

Disclosure or sharing may include, but is not limited to:

- Submission of reports to the Commission on Higher Education (CHED);
- Compliance with requests from authorized government agencies;
- Coordination with scholarship-granting institutions and funding agencies;
- Academic partnerships and collaborative programs; and
- Engagement of authorized service providers performing functions on behalf of the college.

7. Retention

Personal data shall be retained only for as long as necessary to fulfill the purposes for which they were collected and processed or as required by law and institutional policies.

Records subject to retention may include the following, but are not limited to:

- Academic and scholastic records;
- Enrollment and admission documents;
- Scholarship and financial assistance records;
- Research and extension records;
- Administrative and financial records; and
- Other records subject to applicable retention schedules.

8. Disposal and Destruction

Personal data that are no longer necessary for legitimate institutional purposes and are no longer required by law to be retained shall be securely disposed of or destroyed.

Methods for the disposal and destruction of personal data may include, but are not limited to:

- Shredding, pulping, or incineration of paper records;
- Secure deletion of electronic files and databases;
- Overwriting, degaussing, or sanitization of digital storage media;

- Physical destruction of storage devices; and
- Other approved methods that render personal data unreadable, irretrievable, and incapable of reconstruction.

This creates a uniform drafting style throughout the entire Data Life Cycle section and reads more like a formal university policy manual.

B. Data Privacy Principles

The City College of Cagayan de Oro recognizes that privacy protection is founded upon the principles of transparency, legitimate purpose, and proportionality.

1. Transparency

Students, parents, and guardians shall be informed of the nature, purpose, and extent of the processing of their personal data, including their rights as data subjects and the safeguards adopted by the College.

2. Legitimate Purpose

Personal information shall be processed only for lawful and legitimate purposes consistent with the educational mandate of the college and applicable laws and regulations.

3. Proportionality

The processing of personal data shall be adequate, relevant, suitable, and not excessive in relation to the declared purpose for which such information is collected.

C. Categories of Personal Data Processed

In the performance of its educational, administrative, research, extension, and public service functions, the City College of Cagayan de Oro (CCCDO) may collect, process, and maintain various categories of personal data necessary for legitimate institutional purposes. The categories of personal data processed by the College include, but are not limited to, the following:

1. Student Information

Student information refers to personal data relating to applicants, enrolled students, graduates, and alumni of the college. Such information may include, but is not limited to, names, demographic information, contact details, educational background, enrollment records, student identification information, and other information necessary for the delivery of educational services.

2. Parent and Guardian Information

The College may process information relating to parents, guardians, or authorized representatives of students for purposes relating to student welfare, emergency response, communication, parental engagement, and compliance with institutional and legal requirements. Such information may include names, addresses, contact information, and relationships to the student.

3. Sensitive Personal Information

The College may process sensitive personal information when authorized by law or when necessary for legitimate institutional purposes. Such information may include, but is not limited to, health records, disability-related information, government-issued identification numbers, financial assistance eligibility information, and other information classified as sensitive personal information under applicable privacy laws.

4. Academic Records

Academic records refer to information relating to a student's educational performance and academic history. Such records may include, but are not limited to, admission records, enrollment records, class schedules, grades, academic standing, examination results, graduation records, awards, honors, and disciplinary records.

5. Electronic Data

The College may process electronic data generated through the use of institutional information systems, websites, applications, learning management systems, communication platforms, and other digital technologies. Such information may include, but is not limited to, usernames, login credentials, internet protocol (IP) addresses, system logs, electronic communications, online activity records, and other system-generated information.

D. Purposes of Processing

The City College of Cagayan de Oro processes personal data only for lawful, legitimate, and specific purposes consistent with its mandate as a higher education institution. Personal data shall be processed only to the extent necessary to fulfill educational, administrative, regulatory, and public service functions.

1. Admission and Enrollment

Personal data may be processed to evaluate applications, verify qualifications, establish student records, facilitate enrollment, and manage academic registration processes.

2. Academic Administration

Personal data may be processed to administer academic programs, evaluate academic performance, maintain scholastic records, issue academic credentials, and support other academic functions of the college.

3. Student Affairs and Services

Personal data may be processed to administer programs and services relating to student development, student organizations, leadership activities, guidance and counseling, disciplinary processes, cultural activities, sports development, and other student welfare initiatives.

4. Research

Personal data may be processed for research, surveys, institutional studies, and other scholarly activities conducted in accordance with applicable ethical, legal, and institutional requirements.

5. Scholarships and Financial Assistance

Personal data may be processed to evaluate eligibility and administer scholarships, grants, educational assistance, tuition subsidies, and other student financial support programs.

6. Health and Wellness Services

Personal data may be processed to provide medical, dental, psychological, counseling, emergency, and other health-related services intended to promote the welfare and well-being of students.

7. Security and Safety

Personal data may be processed to protect students, personnel, visitors, facilities, information systems, and other institutional assets through the implementation of security, emergency response, and risk management measures.

8. CHED and Government Reporting

Personal data may be processed to comply with reporting, accreditation, quality assurance, audit, records management, scholarship administration, and other regulatory requirements imposed by the Commission on Higher Education (CHED), the National Privacy Commission (NPC), the city government of Cagayan de Oro, and other authorized government agencies.

PART III
LAWFUL PROCESSING OF PERSONAL DATA

A. Lawful Bases for Processing

The City College of Cagayan de Oro (CCCDO) shall process personal data only when authorized by law and when a lawful basis for processing exists. All processing activities undertaken by the College shall comply with the principles of transparency, legitimate purpose, and proportionality as provided under the Data Privacy Act of 2012 and its Implementing Rules and Regulations.

Personal data may be processed on the basis of consent, compliance with legal obligations, performance of contractual obligations, protection of vital interests, fulfillment of public functions, pursuit of legitimate institutional interests, and other lawful bases recognized under applicable laws and regulations. The College shall ensure that every processing activity is supported by an appropriate legal basis and is limited to what is necessary to accomplish legitimate institutional purposes.

B. Consent

Whenever required by law, the College shall obtain the consent of the data subject prior to the collection and processing of personal data. Consent shall be freely given, specific, informed, and evidenced by written, electronic, or recorded means.

The College shall provide data subjects with sufficient information regarding the nature, purpose, scope, and consequences of processing before obtaining consent. Data subjects shall likewise be informed of their rights under applicable privacy laws and shall be given the opportunity to withdraw consent whenever legally permissible.

For students who are minors, consent may be obtained from a parent, legal guardian, or authorized representative in accordance with applicable laws and regulations.

C. Processing Without Consent

The College may process personal data without obtaining consent when such processing is authorized or required by law or when another lawful basis exists under the Data Privacy Act of 2012.

Processing without consent may be undertaken in circumstances including, but not limited to:

- Compliance with legal obligations imposed upon the College;
- Fulfillment of the College's mandate as a public higher education institution;
- Performance of contractual obligations involving the data subject;
- Protection of the life, health, safety, or vital interests of a data subject or another person;
- Compliance with lawful orders of courts, regulatory agencies, and government authorities;
- Reporting requirements imposed by the Commission on Higher Education (CHED), the National Privacy Commission (NPC), UniFAST, and other authorized government agencies; and
- Other instances permitted under applicable laws and regulations.

The College shall ensure that processing without consent remains lawful, necessary, and proportionate to the purpose for which the information is processed.

D. Processing of Sensitive Personal Information

The College recognizes that certain categories of personal data require a higher degree of protection due to their confidential and sensitive nature. Sensitive personal information shall be processed only when authorized by law and when appropriate safeguards are in place to protect the rights and interests of data subjects.

Sensitive personal information processed by the College may include, but is not limited to:

- Health, medical, dental, and psychological records;
- Disability-related information;
- Government-issued identification numbers;
- Information relating to scholarships and financial assistance programs;
- Information required to provide special accommodations, student support services, or welfare interventions; and
- Other information classified as sensitive personal information under applicable laws and regulations.

Access to sensitive personal information shall be restricted to authorized personnel whose official duties require such access and shall be subject to enhanced security and confidentiality measures.

E. Processing of Student Records

The College may process student records as necessary for the administration of academic programs, student services, institutional operations, and compliance with legal and regulatory requirements.

Student records may include the following, but are not limited to:

- Admission and enrollment records;
- Academic transcripts and scholastic records;
- Class schedules and course registrations;
- Grades, examination results, and academic standing;
- Graduation and credential records;
- Student affairs and disciplinary records;
- Scholarship and financial assistance records; and
- Other records necessary for the delivery of educational services.

The processing of student records shall be limited to authorized purposes and shall be subject to appropriate safeguards designed to ensure their confidentiality, integrity, and availability.

F. Processing of Parent and Guardian Information

The College may process personal data relating to parents, guardians, or authorized representatives when such processing is necessary to support student welfare, academic administration, communication, emergency response, financial assistance programs, and other legitimate institutional functions.

Parent and guardian information processed by the College may include, but is not limited to:

- Names and relationship to the student;
- Residential and mailing addresses;
- Telephone numbers and email addresses;
- Emergency contact information;
- Financial information required for scholarship and assistance programs; and
- Other information necessary for the protection of the interests and welfare of students.

The College shall ensure that parent and guardian information is processed only for lawful and legitimate purposes and shall adopt appropriate measures to safeguard such information from unauthorized access, disclosure, alteration, or misuse.

PART IV
ACCESS, DISCLOSURE, AND DATA SHARING

The City College of Cagayan de Oro (CCCDO) recognizes the importance of ensuring that access to, disclosure of, and sharing of personal data are conducted in a lawful, secure, and accountable manner. The College shall implement appropriate safeguards to ensure that personal data are accessed, disclosed, and shared only for legitimate institutional purposes and in accordance with applicable laws, regulations, and institutional policies.

A. Access to Personal Data

Access to personal data shall be restricted to authorized personnel whose official duties and responsibilities require such access. The College shall adopt appropriate access control measures to ensure that personal data are protected against unauthorized use, disclosure, modification, or destruction.

Access privileges shall be granted based on the principle of least privilege and shall be periodically reviewed to ensure that access remains necessary and appropriate. Individuals granted access to personal data shall be required to observe confidentiality obligations and comply with applicable privacy and information security policies.

B. Internal Sharing of Personal Data

The College may share personal data among its academic, administrative, and support offices when necessary for the performance of institutional functions and the delivery of services to students, parents, guardians, and other stakeholders.

Internal sharing may include, but is not limited to:

- Admission, enrollment, and registration processes;
- Academic administration and student records management;
- Scholarship and financial assistance administration;
- Guidance, counseling, health, and wellness services;
- Student affairs and disciplinary proceedings;
- Institutional planning, monitoring, and evaluation; and

- Other legitimate activities necessary for the effective operation of the college.

All internal sharing shall be limited to information necessary for the intended purpose and shall be subject to appropriate confidentiality and security controls.

C. External Disclosure and Data Sharing

The college may disclose or share personal data with external parties when authorized by law, required for the performance of legitimate institutional functions, necessary to protect the interests of data subjects, or with the consent of the data subject when required.

External disclosure or data sharing may include, but is not limited to:

- Government agencies and regulatory authorities;
- Scholarship-granting institutions and funding agencies;
- Accrediting bodies and quality assurance organizations;
- Partner educational institutions;
- Research collaborators;
- Service providers engaged by the College; and
- Other entities authorized by law or by the data subject.

The College shall ensure that all external disclosures and data-sharing activities are supported by a lawful basis and are conducted in accordance with applicable privacy and security requirements.

D. Third-Party Processing

The College may engage third-party service providers to process personal data on its behalf for purposes consistent with its educational, administrative, operational, and technological requirements.

Third-party processing activities may include the following, but are not limited to:

- Information technology and cloud-based services;
- Learning management systems and educational platforms;
- Data storage and backup services;
- Records digitization and document management services;
- Communication and notification services; and
- Other services necessary for institutional operations.

The College shall ensure that third-party processors implement appropriate organizational, physical, and technical safeguards to protect personal data and comply with applicable data privacy obligations.

E. Data Sharing Agreements

Whenever required by law, regulation, or institutional policy, the College shall enter into appropriate Data Sharing Agreements (DSAs), outsourcing agreements, or similar contractual arrangements governing the sharing or processing of personal data.

Such agreements shall establish the purpose of the sharing, the responsibilities of the parties, applicable security measures, confidentiality requirements, retention periods, procedures for incident reporting, and other provisions necessary to ensure the protection of personal data.

The College, through the Technology Innovation and Data Management Center (TIDMAC), the Data Protection Officer, and concerned offices, shall ensure that data-sharing arrangements comply with applicable laws and regulations.

F. Research and Statistical Use

Personal data may be processed for research, statistical analysis, institutional studies, policy development, and quality improvement initiatives, provided that such processing is conducted in accordance with applicable ethical standards, privacy laws, and institutional policies.

Whenever practicable, personal data used for research and statistical purposes shall be anonymized, pseudonymized, aggregated, or otherwise processed in a manner that minimizes privacy risks and protects the identity of data subjects.

Researchers, faculty members, students, and other individuals involved in research activities shall observe appropriate confidentiality and data protection measures throughout the research process.

G. Government Reporting Requirements

The College may process, disclose, and share personal data as necessary to comply with reporting, monitoring, audit, accreditation, quality assurance, scholarship administration, and other regulatory requirements imposed by authorized government agencies.

Such disclosures may include, but are not limited to, submissions to:

- The Commission on Higher Education (CHED);
- Higher Education Management Information System (HEMIS);
- Unified Student Financial Assistance System for Tertiary Education (UniFAST);
- Tertiary Education Subsidy (TES) Program;
- National Privacy Commission (NPC);
- Commission on Audit (COA);
- Civil Service Commission (CSC);
- City Government of Cagayan de Oro; and
- Other government agencies authorized by law.

The College shall ensure that disclosures made pursuant to government reporting requirements are limited to information necessary to comply with legal and regulatory obligations and are protected through appropriate safeguards.

PART V
SECURITY MEASURES

The City College of Cagayan de Oro (CCCDO) shall implement appropriate organizational, physical, and technical measures to protect personal data against unauthorized access, disclosure, alteration, destruction, misuse, loss, or any other unlawful processing. Through the Technology Innovation and Data Management Center (TIDMAC), the Data Protection Officer, and concerned offices, the college shall continuously strengthen its information security and privacy protection practices in accordance with applicable laws, regulations, and recognized standards.

A. Organizational Security Measures

The College shall establish policies, procedures, and governance mechanisms designed to ensure compliance with data privacy and information security requirements. Roles and responsibilities relating to personal data protection shall be clearly defined and communicated to all personnel.

Organizational measures may include the following, but are not limited to:

- Adoption of privacy and information security policies;
- Designation of a Data Protection Officer;
- Establishment of access control procedures;
- Employee confidentiality undertakings;
- Privacy awareness programs; and

- Regular compliance reviews and assessments.

B. Physical Security Measures

The College shall implement physical safeguards to protect facilities, equipment, records, and storage areas containing personal data from unauthorized access, theft, damage, or destruction.

Physical security measures may include the following, but are not limited to:

- Controlled access to offices and records storage areas;
- Visitor monitoring procedures;
- Locked filing cabinets and storage facilities;
- Security personnel and surveillance systems;
- Environmental controls for records preservation; and
- Secure disposal facilities for confidential records.

C. Technical Security Measures

The College shall implement appropriate technical controls to secure electronic records, databases, networks, information systems, and digital platforms that process personal data.

Technical security measures may include the following, but are not limited to:

- User authentication and password controls;
- Role-based access controls;
- Encryption technologies;
- Firewalls and network security systems;
- Data backup and recovery mechanisms;
- Anti-malware and endpoint protection solutions; and
- Security monitoring and vulnerability management tools.

D. Security Incident Prevention and Monitoring

The College shall adopt preventive measures to identify, monitor, and address potential security threats affecting personal data and institutional information assets.

Security monitoring activities may include the following, but are not limited to:

- Risk assessments;
- System monitoring and logging;
- Vulnerability assessments;

- Security audits;
- Incident detection mechanisms; and
- Continuous review of information security controls.

E. Confidentiality and Non-Disclosure Obligations

All officials, faculty members, employees, students, consultants, service providers, and other authorized persons who have access to personal data shall maintain the confidentiality of such information and shall use it only for authorized purposes.

Access to personal data shall not be disclosed, shared, copied, or otherwise processed beyond authorized purposes except as permitted by law or institutional policy. Confidentiality obligations shall continue even after separation from service, graduation, completion of contracts, or termination of affiliation with the College.

PART VI
RIGHTS OF DATA SUBJECTS

The City College of Cagayan de Oro recognizes and respects the rights of data subjects under the Data Privacy Act of 2012 and related issuances of the National Privacy Commission. Students, parents, guardians, employees, and other individuals whose personal data are processed by the College shall be entitled to exercise the rights provided by law, subject to applicable limitations and exceptions.

A. Right to Be Informed

Data subjects shall have the right to be informed whether personal data pertaining to them are being processed, the purposes of processing, the legal basis thereof, the recipients of the information, and other relevant details relating to the processing of their personal data.

B. Right to Access

Data subjects shall have the right to obtain reasonable access to their personal data and information regarding the manner by which such data have been processed, subject to applicable legal and institutional restrictions.

C. Right to Object

Data subjects shall have the right to object to the processing of their personal data, including processing for direct marketing, automated processing, or other purposes not authorized by law, subject to lawful and legitimate grounds for continued processing.

D. Right to Rectification

Data subjects shall have the right to dispute inaccuracies or errors in their personal data and request the correction, updating, or completion of such information.

E. Right to Erasure or Blocking

Data subjects shall have the right to request the suspension, withdrawal, blocking, removal, or destruction of personal data when permitted by law and when the information is incomplete, outdated, false, unlawfully obtained, or no longer necessary for the purpose for which it was collected.

F. Right to Data Portability

Data subjects shall have the right to obtain and electronically transfer their personal data in a structured and commonly used format, subject to technical feasibility and applicable legal requirements.

G. Right to Damages

Data subjects who suffer damages arising from inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal data may seek compensation and other remedies available under applicable laws.

H. Right to File a Complaint

Data subjects shall have the right to lodge complaints with the College, the Data Protection Officer, the National Privacy Commission, or other appropriate authorities concerning alleged violations of their privacy rights or applicable data protection laws.

PART VII
DATA BREACH MANAGEMENT

The City College of Cagayan de Oro (CCCDO) recognizes the importance of promptly detecting, assessing, reporting, and responding to security incidents and personal data breaches. The College shall establish appropriate procedures to minimize risks to data subjects, protect institutional information assets, and ensure compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and relevant issuances of the National Privacy Commission (NPC), including NPC Circular No. 16-03 on Personal Data Breach Management.

Through the Technology Innovation and Data Management Center (TIDMAC), the Data Protection Officer (DPO), and concerned offices, the College shall maintain a coordinated breach management program designed to identify, contain, investigate, mitigate, and prevent incidents involving personal data.

A. Definition of Security Incident

A security incident refers to an event or occurrence that affects or may affect the confidentiality, integrity, or availability of personal data, information systems, records, networks, or other information assets of the college.

Security incidents may include, but are not limited to:

- Unauthorized access attempts;
- Malware infections;
- Loss or theft of devices containing personal data;
- Accidental disclosure of information;
- System failures affecting data availability;
- Unauthorized alteration of records; and
- Other events that may compromise information security.

Not all security incidents constitute personal data breaches. However, all security incidents shall be appropriately documented, assessed, and addressed.

B. Definition of Personal Data Breach

A personal data breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed by the College.

Personal data breaches may involve:

- Unauthorized disclosure of student records;
- Exposure of personal information through electronic systems;
- Loss or theft of records containing personal data;
- Improper access to confidential information;
- Accidental publication of personal information; and
- Other incidents resulting in the compromise of personal data.

C. Reporting Procedures

All officials, employees, faculty members, students, contractors, service providers, and other authorized persons who become aware of a security incident or suspected personal data breach shall immediately report the matter to their immediate supervisor, the Technology Innovation and Data Management Center (TIDMAC), the Data Protection Officer, or other designated authorities within the college.

Reports shall include available information regarding:

- The nature of the incident;
- The date and time of discovery;
- The systems, records, or information involved;
- The number and categories of affected individuals, if known; and
- Any actions already taken to address the incident.

The College shall maintain appropriate mechanisms for reporting and documenting security incidents and personal data breaches.

D. Breach Assessment and Containment

Upon receipt of a report, the College shall promptly conduct an assessment to determine the nature, scope, severity, and potential impact of the incident.

Assessment activities may include, but are not limited to:

- Verification of the incident;
- Identification of affected data and systems;
- Determination of the number of affected data subjects;
- Evaluation of potential risks and harms;
- Preservation of evidence; and
- Immediate implementation of containment measures.

The College shall take reasonable steps to prevent further unauthorized access, disclosure, alteration, or loss of personal data while the incident is being investigated.

E. Notification to the National Privacy Commission

Where required by law and applicable regulations, the College shall notify the National Privacy Commission of a personal data breach within the period prescribed by applicable rules.

Such notification shall contain all information required by the National Privacy Commission, including details regarding the nature of the breach, affected data subjects, likely consequences, and measures undertaken to address the incident.

The Data Protection Officer shall coordinate the preparation and submission of breach notifications to the National Privacy Commission.

F. Notification to Affected Data Subjects

When a personal data breach is likely to result in a risk to the rights and freedoms of affected individuals, the College shall notify affected data subjects in accordance with applicable laws and regulations.

Notifications shall be made through appropriate means and shall contain information including, but not limited to:

- The nature of the breach;
- The personal data involved;
- The potential consequences of the breach;
- Measures taken by the College;
- Recommended actions for affected individuals; and
- Contact information for further assistance.

The College shall endeavor to provide notifications as promptly as circumstances permit.

G. Corrective, Mitigating, and Preventive Measures

Following a security incident or personal data breach, the College shall implement appropriate corrective, mitigating, and preventive measures to reduce risks and prevent recurrence.

Such measures may include, but are not limited to:

- System restoration and recovery;
- Password resets and access control modifications;
- Security enhancements and software updates;

- Revision of policies and procedures;
- Employee retraining and awareness activities;
- Strengthening of technical and organizational safeguards; and
- Other measures deemed necessary to improve information security and privacy protection.

The College shall document all breach management activities and may conduct post-incident reviews to identify lessons learned and opportunities for continuous improvement.

PART VIII
RECORDS RETENTION, ARCHIVING, DISPOSAL, AND DESTRUCTION

The City College of Cagayan de Oro (CCCDO) recognizes the importance of maintaining accurate, reliable, and accessible records while ensuring the protection of personal data throughout their retention period. The College shall establish and implement records retention, archiving, disposal, and destruction practices consistent with the Data Privacy Act of 2012, Republic Act No. 9470 or the National Archives of the Philippines Act of 2007, applicable records management regulations, Commission on Higher Education (CHED) requirements, and institutional policies.

Personal data shall be retained only for as long as necessary to fulfill legitimate institutional purposes, comply with legal obligations, protect the rights of data subjects, and support the operational requirements of the college.

A. Records Retention Schedule

The college shall maintain and implement records retention schedules that prescribe the period during which records containing personal data shall be retained.

Retention periods shall be determined based on:

- Applicable laws and regulations;
- Records management requirements;
- Academic and administrative needs;
- Audit and accountability requirements;
- Research and historical value; and
- Other legitimate institutional purposes.

Records subject to retention may include the following, but are not limited to:

- Admission and enrollment records;
- Academic and scholastic records;

- Graduation and credential records;
- Scholarship and financial assistance records;
- Personnel and administrative records;
- Research and extension records; and
- Financial and audit-related records.

The College shall periodically review retention schedules to ensure continued compliance with applicable legal and institutional requirements.

B. Records Archiving

Records that are no longer actively used but remain subject to retention requirements may be transferred to archival storage in accordance with approved records management procedures.

Archived records may include the following, but are not limited to:

- Historical academic records;
- Institutional reports and publications;
- Research outputs and documentation;
- Accreditation and quality assurance records;
- Administrative and governance records; and
- Other records possessing continuing administrative, legal, fiscal, evidentiary, or historical value.

The College shall implement appropriate safeguards to preserve the integrity, confidentiality, authenticity, and accessibility of archived records.

C. Disposal of Records

Records containing personal data that have reached the end of their approved retention period and no longer possess administrative, legal, fiscal, research, or historical value may be disposed of in accordance with approved records management procedures.

Prior to disposal, the college shall ensure that:

- Applicable retention periods have expired;
- No pending investigation, audit, litigation, or administrative proceeding requires continued retention;
- Necessary approvals have been obtained from authorized offices; and
- Applicable records management requirements have been satisfied.

The disposal of records shall be properly documented to ensure accountability and compliance with applicable laws and regulations.

D. Secure Destruction of Personal Data

Personal data that are no longer required for legitimate institutional purposes and are authorized for destruction shall be destroyed using secure methods designed to prevent unauthorized access, disclosure, retrieval, reconstruction, or reuse.

Methods for the secure destruction of personal data may include, but are not limited to:

- Shredding, pulping, or incineration of paper records;
- Secure deletion of electronic records and databases;
- Overwriting, degaussing, or sanitization of digital storage media;
- Physical destruction of storage devices; and
- Other approved methods consistent with applicable records management, information security, and data privacy standards.

The College shall ensure that destruction activities are properly documented and conducted under appropriate supervision. Records of disposal and destruction shall be maintained to demonstrate compliance with legal, regulatory, and institutional requirements.

PART IX
PRIVACY GOVERNANCE AND ACCOUNTABILITY

The City College of Cagayan de Oro (CCCDO) recognizes that the protection of personal data is a shared institutional responsibility. The College shall establish and maintain an effective privacy governance framework that promotes accountability, transparency, compliance, and responsible stewardship of personal data throughout the institution.

All officials, employees, faculty members, students, service providers, and other persons authorized to process personal data on behalf of the college shall comply with applicable privacy laws, regulations, and institutional policies. The College shall ensure that responsibilities relating to privacy protection and information security are clearly defined and appropriately implemented.

A. General Responsibilities

All members of the college community who collect, access, use, disclose, store, transmit, retain, or otherwise process personal data shall be responsible for protecting such information and ensuring compliance with this Privacy Policy.

General responsibilities include, but are not limited to:

- Processing personal data only for authorized purposes;
- Protecting personal data against unauthorized access, disclosure, alteration, or destruction;
- Reporting security incidents and personal data breaches;
- Observing confidentiality obligations;
- Participating in privacy and information security programs; and
- Complying with applicable laws, regulations, and institutional policies.

B. Technology Innovation and Data Management Center (TIDMAC)

The Technology Innovation and Data Management Center (TIDMAC) shall serve as the college's primary office for information governance, technology innovation, digital transformation, information security, and institutional data management.

TIDMAC shall support the implementation of this Privacy Policy and shall coordinate institutional efforts relating to privacy protection, cybersecurity, records digitization, information systems management, and data governance.

Its responsibilities may include the following, but are not limited to:

- Developing and recommending privacy and information security policies;
- Managing and securing institutional information systems and databases;
- Supporting compliance with privacy laws and regulations;
- Monitoring information security risks and vulnerabilities;
- Coordinating responses to security incidents and personal data breaches;
- Promoting responsible data governance and digital innovation; and
- Performing other functions necessary to strengthen institutional privacy and information security.

C. Data Protection Officer

The college shall designate a Data Protection Officer (DPO) in accordance with the requirements of the Data Privacy Act of 2012 and applicable National Privacy Commission issuances.

The DPO shall oversee and monitor the College's compliance with privacy laws and regulations and shall serve as the primary contact person for privacy-related concerns.

The responsibilities of the DPO may include the following, but are not limited to:

- Monitoring compliance with privacy laws and institutional policies;
- Advising management on privacy-related matters;
- Coordinating privacy compliance initiatives;
- Conducting privacy impact assessments and compliance reviews;
- Receiving and addressing privacy-related complaints and concerns;
- Coordinating personal data breach management activities; and
- Serving as liaison with the National Privacy Commission and other relevant authorities.

D. Information Technology Personnel

Information technology personnel shall be responsible for implementing, maintaining, and monitoring technical safeguards designed to protect institutional information systems and personal data.

Their responsibilities may include the following, but are not limited to:

- Managing system access controls;
- Maintaining network and information security measures;
- Monitoring system performance and security events;
- Performing backup and recovery activities;
- Implementing software updates and security patches;
- Assisting in incident response and system recovery; and
- Supporting privacy and cybersecurity initiatives.

E. Academic and Administrative Offices

Academic and administrative offices that collect, maintain, or process personal data shall ensure that such information is handled in accordance with applicable laws and institutional policies.

Their responsibilities may include the following, but are not limited to:

- Maintaining accurate and reliable records;
- Ensuring lawful processing of personal data;
- Limiting access to authorized personnel;

- Implementing office-level security measures;
- Supporting privacy compliance initiatives; and
- Cooperating with audits, investigations, and compliance reviews.

F. Faculty Members and Employees

Faculty members and employees who process personal data in the performance of their duties shall exercise due care and diligence in protecting such information.

Their responsibilities may include the following, but are not limited to:

- Maintaining confidentiality of personal data;
- Using information only for authorized purposes;
- Protecting records under their custody;
- Reporting security incidents and privacy concerns;
- Participating in privacy and cybersecurity training activities; and
- Complying with applicable laws and institutional policies.

G. Students, Parents, and Guardians

Students, parents, and guardians shall contribute to the protection of personal data by providing accurate information, exercising their privacy rights responsibly, and complying with applicable college policies relating to the use of information systems and institutional records.

They are encouraged to:

- Safeguard personal credentials and account information;
- Promptly report inaccuracies in records;
- Notify the College of suspected privacy violations;
- Exercise their rights as data subjects responsibly; and
- Cooperate with legitimate institutional processes involving personal data.

H. Service Providers and Third Parties

Service providers, contractors, consultants, partner institutions, and other third parties that process personal data on behalf of the College shall comply with applicable privacy laws, contractual obligations, and institutional requirements.

Such parties shall be required to implement appropriate organizational, physical, and technical safeguards to protect personal data and shall process information only for authorized purposes consistent with applicable agreements and legal requirements.

The College may require third parties to execute confidentiality agreements, data-sharing agreements, outsourcing agreements, or other instruments necessary to ensure the protection of personal data entrusted to them.

PART X
TRAINING, AWARENESS, AND COMPLIANCE

The City College of Cagayan de Oro (CCCDO) recognizes that effective privacy protection requires continuous education, awareness, and compliance efforts throughout the institution. The College shall promote a culture of privacy, accountability, and responsible data management by providing appropriate training programs, awareness initiatives, compliance monitoring activities, and regular assessments of privacy practices.

Through the Technology Innovation and Data Management Center (TIDMAC), the Data Protection Officer (DPO), and other concerned offices, the College shall develop and implement programs designed to strengthen privacy awareness, enhance data protection capabilities, and ensure compliance with applicable laws, regulations, and institutional policies.

A. Privacy Awareness Programs

The College shall conduct privacy awareness activities to promote understanding of data privacy principles, data subject rights, information security practices, and institutional responsibilities relating to the protection of personal data.

Privacy awareness activities may include the following, but are not limited to:

- Information campaigns and dissemination activities;
- Privacy awareness seminars and orientations;
- Distribution of privacy advisories and educational materials;
- Data Privacy Week and similar institutional activities;
- Awareness programs for students, parents, and guardians; and
- Other initiatives designed to promote responsible data management practices.

The College shall endeavor to ensure that privacy awareness activities are conducted regularly and are accessible to members of the academic community.

B. Capacity Building and Training

The College shall provide appropriate privacy and information security training to officials, faculty members, employees, student leaders, and other individuals who process personal data in the performance of their duties.

Training programs may include the following, but are not limited to:

- Fundamentals of data privacy and protection;
- Data Privacy Act of 2012 and related regulations;
- Information security and cybersecurity awareness;
- Secure handling of personal and sensitive personal information;
- Data breach reporting and incident response procedures;
- Records management and information governance practices; and
- Role-specific privacy and security responsibilities.

The frequency and scope of training activities shall be determined based on operational needs, risk considerations, and applicable regulatory requirements.

C. Monitoring and Compliance Activities

The College shall establish mechanisms to monitor compliance with privacy laws, regulations, institutional policies, and information security requirements.

Compliance activities may include, but are not limited to:

- Internal compliance reviews;
- Policy implementation assessments;
- Security monitoring activities;
- Documentation and records inspections;
- Verification of compliance with privacy requirements;
- Review of data processing activities; and
- Other measures necessary to evaluate institutional compliance.

The college may require offices and personnel to cooperate in compliance monitoring activities and provide information necessary to assess adherence to privacy requirements.

D. Privacy Impact Assessments and Audits

The college may conduct Privacy Impact Assessments (PIAs), privacy audits, information security assessments, and related evaluations to identify privacy risks, assess compliance obligations, and strengthen data protection practices.

Such assessments may include, but are not limited to:

- Evaluation of new programs, projects, systems, or technologies;
- Assessment of data processing activities involving personal data;
- Review of privacy and information security controls;
- Identification and management of privacy risks;
- Verification of compliance with legal and regulatory requirements; and
- Development of corrective and improvement measures.

Results of privacy impact assessments, audits, and related evaluations shall be used to improve institutional policies, procedures, safeguards, and compliance programs. The College shall take appropriate action to address identified risks, vulnerabilities, and areas requiring improvement.

All members of the college community shall cooperate with privacy assessments, audits, inspections, and compliance activities authorized by the college and conducted in accordance with applicable laws and institutional policies.

PART XI
COMPLAINTS AND GRIEVANCE MECHANISM

The City College of Cagayan de Oro (CCCDO) recognizes the right of data subjects to seek redress for concerns relating to the processing of their personal data. The College shall establish accessible, fair, and transparent procedures for receiving, investigating, resolving, and monitoring privacy-related complaints and grievances.

Complaints shall be handled in a timely, impartial, and confidential manner, consistent with applicable laws, regulations, and institutional policies.

A. Filing of Complaints

Any student, parent, guardian, employee, applicant, visitor, or other data subject who believes that their privacy rights have been violated may file a complaint with the College through the Data Protection Officer (DPO), the Technology Innovation and Data Management Center (TIDMAC), or other authorized offices.

Complaints may include, but are not limited to:

- Unauthorized collection of personal data;
- Unauthorized access, disclosure, or sharing of personal information;
- Inaccurate or incomplete records;
- Failure to respect data subject rights;
- Security incidents involving personal data; and

- Other alleged violations of privacy laws, regulations, or institutional policies.

Complaints shall, whenever practicable, contain sufficient information to facilitate investigation and resolution.

B. Investigation Procedures

Upon receipt of a complaint, the College shall conduct an appropriate review and investigation of the matter.

Investigation activities may include, but are not limited to:

- Verification of the facts and circumstances;
- Review of relevant records and documentation;
- Interviews with concerned parties;
- Assessment of applicable laws, regulations, and policies; and
- Determination of appropriate corrective actions.

The College shall ensure that investigations are conducted fairly, objectively, and with due regard for the rights of all parties involved.

C. Resolution of Complaints

Following the investigation, the College shall take appropriate action to address the complaint and prevent the recurrence of similar incidents.

Resolution measures may include, but are not limited to:

- Correction or updating of records;
- Restriction or suspension of unauthorized processing activities;
- Implementation of additional safeguards;
- Provision of appropriate remedies to affected individuals;
- Referral to appropriate offices for disciplinary action; and
- Other lawful and appropriate corrective measures.

The complainant shall be informed of the outcome of the investigation and the actions taken by the college, subject to applicable confidentiality and legal considerations.

D. Appeals and Escalation

A complainant who is dissatisfied with the resolution of a complaint may request reconsideration or elevate the matter to higher authorities within the college in accordance with applicable procedures.

Nothing in this Policy shall prevent a data subject from seeking appropriate remedies before the National Privacy Commission or other competent authorities as provided by law.

PART XII
SANCTIONS AND PENALTIES

The City College of Cagayan de Oro (CCCDO) shall hold accountable any individual or entity that violates this Privacy Policy, applicable privacy laws, information security requirements, or other related institutional policies.

The imposition of sanctions and penalties shall be without prejudice to any civil, criminal, administrative, or regulatory liabilities provided under applicable laws.

A. Administrative Sanctions

Violations of this policy may subject responsible individuals to administrative sanctions in accordance with applicable laws, civil service rules, college policies, contractual obligations, and other relevant regulations.

Administrative sanctions may include, but are not limited to:

- Written reprimand;
- Suspension of privileges;
- Administrative penalties;
- Removal of access rights;
- Suspension from duties; and
- Other appropriate disciplinary actions.

B. Disciplinary Measures

Faculty members, employees, students, and other members of the college community who violate privacy and information security requirements may be subjected to disciplinary proceedings in accordance with applicable rules and procedures.

Disciplinary measures shall be imposed only after observance of due process and may vary depending on the nature, severity, frequency, and consequences of the violation.

C. Contractual and Third-Party Liability

Contractors, consultants, service providers, partner institutions, and other third parties engaged by the College may be held liable for violations of privacy obligations arising from contractual agreements, data-sharing arrangements, outsourcing agreements, or other applicable instruments.

The college may impose appropriate contractual remedies, including, but not limited to:

- Suspension of services;
- Termination of contracts;
- Recovery of damages;
- Withholding of payments; and
- Other remedies permitted by law or contract.

D. Civil, Criminal, and Regulatory Liability

Nothing in this Policy shall prevent the institution, affected individuals, or competent authorities from pursuing remedies available under applicable laws.

Violations involving personal data may result in civil, criminal, or regulatory liabilities under the Data Privacy Act of 2012 and other applicable laws and regulations.

PART XIII
POLICY REVIEW AND AMENDMENT

The City College of Cagayan de Oro (CCCDO) recognizes that privacy risks, technologies, legal requirements, and institutional operations continuously evolve. Accordingly, this Privacy Policy shall be subject to regular review and updating to ensure its continued relevance, effectiveness, and compliance with applicable laws and regulations.

A. Periodic Review

This Policy shall be reviewed periodically by the Technology Innovation and Data Management Center (TIDMAC), the Data Protection Officer (DPO), and other concerned offices to assess its adequacy, effectiveness, and alignment with legal, regulatory, operational, and technological developments.

Reviews may consider, among others:

- Changes in applicable laws and regulations;
- National Privacy Commission issuances;
- CHED policies and requirements;

- Information security developments;
- Institutional operational changes;
- Audit findings and compliance assessments; and
- Recommendations from stakeholders.

B. Amendment Procedures

Amendments, revisions, or modifications to this policy may be proposed by TIDMAC, the data protection officer, college officials, or other authorized bodies of the institution.

Proposed amendments shall undergo appropriate consultation, review, and approval processes consistent with College governance requirements before implementation.

C. Effect of Amendments

Approved amendments shall form an integral part of this policy and shall take effect on the date specified in the approving authority or implementing issuance.

The college shall undertake reasonable efforts to inform affected stakeholders of significant changes to this policy through appropriate communication channels.

PART XIV
EFFECTIVITY

A. Effectivity Clause

This Privacy Policy for Students, Parents, and Guardians of the City College of Cagayan de Oro shall take effect upon approval by the appropriate college authorities and shall remain in force until amended, revised, or repealed in accordance with applicable laws, regulations, and institutional policies.

B. Repealing Clause

All existing policies, guidelines, procedures, memoranda, and issuances of the College that are inconsistent with the provisions of this Privacy Policy are hereby modified, amended, or repealed accordingly.

C. Separability Clause

If any provision of this Privacy Policy is declared invalid, unconstitutional, or unenforceable by a court or competent authority, the remaining provisions not affected thereby shall continue to remain in full force and effect.

Prepared by:	Approved by:
Jesse James P. Fabela	**Dr. Kurt S. Candilas**
TIDMAC Director	Vice President for Administration and Finance