

J.H. CERILLES STATE COLLEGE
MATI, SAN MIGUEL, ZAMBOANGA DEL SUR
SCHOOL OF LAW

DATA PRIVACY POLICY OF J.H. CERILLES STATE COLLEGE



TABLE CONTENT

Data Privacy of J.H. Cerilles State College	
Rationale.....	1
Covered by the Policy.....	1
Reason of for Processing of Personal Data.....	1
Types of Personal Data Processed.....	2
The Purposes.....	2
Purposes Applicable to all members of JHCSC Community.....	2
Students, Parents and Guardians.....	3
Faculty, Including Visiting Faculty	3
Staff, including Research, Extension and Resources Generation (RERG), JHCSC Contractual, Non- JHCSC Contractual Personnel and Retirees.....	4
Applicant Students, Faculty, and Staff.....	4
Researchers and Research Subjects.....	4
Alumni, Donors and Donees	4
Contract Counterparties, Partners, Subcontractors, Outsources, Licensors, Licensees, Lessors, Lessees, Vendors, Purchaser and Customers	5
Other persons with a juridical link to JHCSC	5
Processing and Retention of Personal Data at JHCSC	5
Storage and Transmission of Personal Data at JHCSC	5
Transmission of Personal Data	6
Rights of JHCSC Community	6
Responsibilities of JHCSC Community	8
Confidentiality Notice Template	9
Effectivity of this Policy	9

Privacy Policy for Students, Parents and Guardians	10
Rationale	10
Definition of Terms	10
Data Collection and Protection of Personal Data	
Of Students, Parents and Guardians.....	11
Data Life Cycle	11
Collection of Personal Data	12
Storage and Transmission of Data	13
Use of Personal Data	13
Academic Purposes.....	13
Extra-Curricular Purposes	13
Medical Purposes	13
Student Assistance Purposes	14
Student Disciplinary Purposes	14
Additional Purposes	14
Retention of Data	14
Disposal and Destruction of Data	15
Data Privacy Principles	15
Transparency	15
Legitimate Purpose	15
Proportionality	16
Security Measures	16
Organizational Security Measures	16
Physical Security Measures	17
Technical Security Measures	17

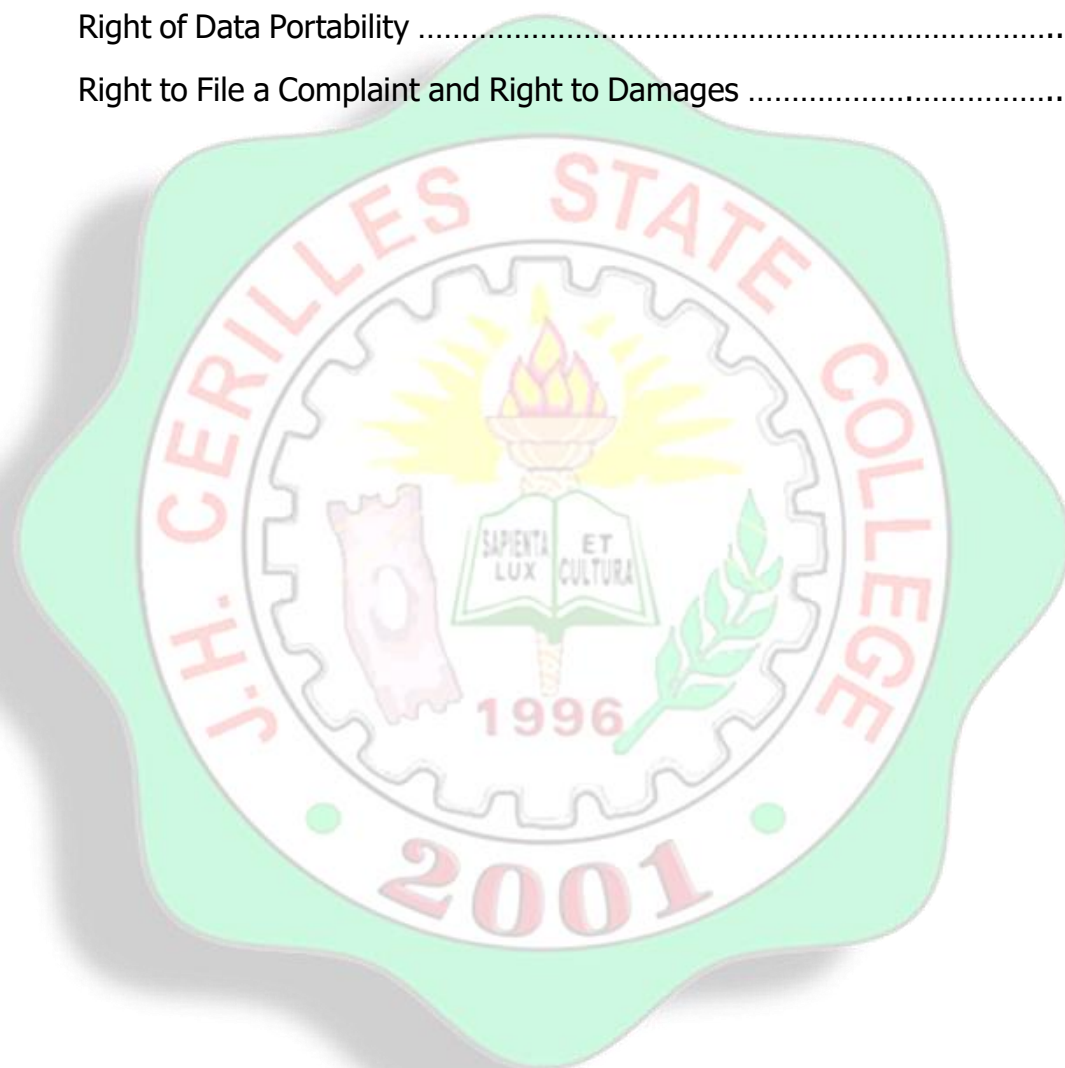
Access to Personal Data	18
Personal Data can be Shared to Other Organization or Institution	18
Personal data can be Access by the Students, Parents, and Guardians	19
Accuracy and Up-To-Date Personal Data	19
Consent	20
Contract Fulfillment	20
Legal Obligation	20
Vital Interest	20
National Emergency and Public Officer	20
Legitimate Interests	20
Rights of Data Subject	21
Right to be Informed	21
Right to Access	21
Right to Object, and Right to Correct or Rectify	21
Right to be Erasure or Blocking	21
Right to Data Portability	21
Right to file a Complaint	21
Right to Damage	22
Privacy Policy for Staff	
Definition of Terms.....	23
Cardinal Principles of Data Privacy in Relation to the Processing of the Staff's Personal Data.....	24
Transparency.....	24
Legitimate Purpose	24

Proportionality.....	25
Processing of Personal Data of Staff.....	25
Collection of Data.....	25
Use of Personal Data.....	26
Storage, Retention, Disposal and Destruction of Personal Data	27
Access	27
Disclosure.....	27
Consent	28
Security Measures.....	28
Organizational Security Measures.....	28
Physical Security Measures.....	28
Technical Security Measures.....	29
Rights of Data Subject.....	29
Right to be Informed.....	29
Right to Access	29
Right to Object and Right to Correct or Rectify	29
Right to Erasure or Blocking	29
Right of Data Portability	30
Right to File a Complaint and Right to Damage	30
Group Chats	31
Privacy Policy for Faculty.....	
Rationale.....	32
Definition of Terms	32
Principles of Data Privacy in Relation to the Processing of the Faculty's Personal Data	33
Transparency	33

Legitimate Purpose	33
Proportionality.....	34
Processing of Personal Data of Faculty	34
Collection of Personal Data	34
Use of Personal Data	35
Storage, Retention, Disposal and Destruction of Personal Data	35
Access	35
Disclosure	36
Consent	36
Security Measures	37
Organizational Security Measures	37
Physical Security Measures	37
Technical Security Measures	37
Rights of Data Subject	37
Right to be Informed	37
Right to Access	38
Right to Object and Right to Correct or Rectify	38
Right to Erasure or Blocking	38
Right of Data Portability	38
Right to File a Complaint and Right to Damages	38
Group Chats.....	39
Privacy Policy for Alumni and Donors	
Rationale	40
Covered by this Policy	40

Reason of Personal Data Processed	40
Types of Personal Data Processed	40
Processing and Retention of Personal Data at JHCSC	41
Personal Data Stored and Transmission	42
Rights and Responsibilities of Alumni and Donor	42
Effectivity and Definition of Terms	42
Data Protection Officer	42
Privacy Policy for Applicant	
Rationale	43
Definition of Terms	43
Principles of Data Privacy in Relation to the Processing of the Applicant's Personal Data	44
Transparency	44
Legitimate Purpose	44
Proportionality	45
Processing of Personal Data	45
Collection of Personal Data	45
Use of Personal Data	46
Storage, Retention, Disposal and Destruction of Personal Data	46
Access	46
Disclosure	47
Consent	47
Security Measures	47
Organizational Security Measures	47
Physical Security Measures	48
Technical Security Measures	48

Rights of Data Subject	48
Right to be Informed	48
Right to Access	48
Right to Object and Right to Correct or Rectify	48
Right to Erasure or Blocking	49
Right of Data Portability	49
Right to File a Complaint and Right to Damages	49



DATA PRIVACY POLICY OF J.H. CERILLES STATE COLLEGE

RATIONALE

The Data Privacy Policy of J.H. Cerilles State College (JHCSC) is established in alignment with the Data Privacy Act of 2012 (Republic Act No. 10173) to safeguard the personal data entrusted to the institution by its students, employees, alumni, and external partners. As a public educational institution, JHCSC is responsible for collecting, storing, and processing various forms of personal information to support its academic, administrative, and operational activities. This policy demonstrates JHCSC's commitment to upholding the privacy and security of personal data by providing a structured framework for handling such information responsibly and transparently.

I. COVERED BY THE POLICY

This Policy applies to students, parents, guardians, faculty, visiting faculty, staff, Research, Extension and Resource Generation (RERG), JHCSC contractual personnel, non-JHCSC contractual personnel, retirees, applicant students, applicant faculty, applicant staff, researchers, research subjects, patients, clients, customers, alumni, donors, donees, contract counterparties, partners, subcontractors, outsourcers, licensors, licensees, and other persons with a juridical link with J.H. Cerilles State College ("JHCSC Community") whose personal information, sensitive personal information, or privileged information ("Personal Data") are processed by J.H. Cerilles State College.

II. REASON FOR PROCESSING OF PERSONAL DATA

(1) Fulfill its obligations, exercise its rights, and conduct its associated functions as:

- an instrumentality of the government;
- a higher educational institution.

(2) Pursue its purposes and mandates as a state college established under Republic Act No. 9151 and any subsequent relevant legislation.

(3) For each specific unit of JHCSC, perform all acts reasonably foreseeable and customarily undertaken by similar institutions.

(4) Make decisions and take actions for the holistic welfare of its students, parents and guardians, faculty, staff, researchers, alumni, and the JHCSC community.

(5) Manage and administer its internal and external affairs as an academic institution, an instrumentality of the government, and a juridical entity with its own rights and interests.

III. TYPES OF PERSONAL DATA PROCESSED

J.H. Cerilles State College (JHCSC) processes Personal Data, including but not limited to:

- Personal details such as name, age, race, ethnic origin, color, date of birth, gender, civil status, religious, philosophical affiliation;
- Contact information such as address, email, mobile, and telephone numbers;
- Academic information such as grades, courses, academic standing, and educational background;
- Employment information such as government-issued numbers, position, functions, and employment history;
- Applicant information such as academic background, previous employment, and other relevant qualifications;
- Medical information such as physical, psychiatric, and psychological information when necessary.

IV. THE PURPOSES

J.H. Cerilles State College (JHCSC) processes Personal Data for the following purposes (the "Purposes"):

(1) Purposes applicable to all members of the JHCSC Community

- 1.1 Purposes necessary for JHCSC to fulfill its obligations, exercise its rights, and carry out functions as a higher education institution and government instrumentality.
- 1.2 Purposes to pursue JHCSC's mandates under Republic Act No. 9151 and other applicable laws.
- 1.3 Purposes to manage JHCSC's internal and external affairs as an academic institution with its rights and interests.
- 1.4 Compliance with legal, regulatory, and administrative requirements, including audit, reporting, and transparency mandates.

- 1.5 Records and account purposes including:
 - 1.5.1. Creation and updating of records and accounts;
 - 1.5.2. Maintenance of student, faculty, and staff records, electronic or otherwise.
- 1.6. Security and community welfare purposes such as:
 - 1.6.1. Ensuring the safety, security, and order in JHCSC campuses and venues;
 - 1.6.2. Crime prevention and property protection within JHCSC's premises.

(2) Students, Parents, and Guardians

- 2.1. Academic purposes, including:
 - 2.1.1. Processing and evaluation of grades for academic decisions;
 - 2.1.2. Formulation, review, and application of JHCSC policies, guidelines, and procedures.
- 2.2. Extra-curricular purposes, including:
 - 2.2.1. Regulation of student organizations;
 - 2.2.2. Collaboration with public and private agencies
- 2.3. Medical purposes, including:
 - 2.3.1. Provision of medical, dental, and psychological services;
 - 2.3.2. Maintaining health records to support patient care.
- 2.4. Student assistance purposes, including:
 - 2.4.1. Provision of scholarships, financial aid, and dormitory services;
 - 2.4.2. Tutoring, mentoring, and internship programs.
- 2.5. Disciplinary purposes, including:
 - 2.5.1. Conducting investigations and hearings on disciplinary matters;
 - 2.5.2. Compliance with relevant laws and orders.

(3) Faculty, including Visiting Faculty

- 3.1. Faculty administration and supervision as JHCSC employees.
- 3.2. Academic and non-academic functions such as:
 - 3.2.1. Assignment of teaching loads, performance evaluations, and promotions;
- 3.3. Managing research, ethics, and intellectual property matters.

(4) Staff, including Research, Extension and Resource Generation (RERG), JHCSC Contractual, Non-JHCSC Contractual Personnel, and Retirees

- 4.1. Human resources management, including:
 - 4.1.1. Processing employee entitlements, compensation, and benefits.
- 4.2. Work supervision and conduct management, including:
 - 4.2.1. Employee assignment, supervision, evaluation, promotion, and discipline;
 - 4.2.2. Maintaining labor relations and workplace harmony.

(5) Applicant Students, Faculty, and Staff

- 5.1. Application processing such as:
 - 5.1.1. Handling applications and requirements;
 - 5.1.2. Evaluating eligibility for enrollment, teaching, or employment at JHCSC.
- 5.2. Verification purposes, including:
 - 5.2.1. Verifying the accuracy of applicant information;
 - 5.2.2. Conducting background checks as relevant to the applied position.

(6) Researchers and Research Subjects

The Exemption from the coverage of Data Privacy Act of 2012 as to personal information used exclusively for scientific and statistical research purposes is in conformance with Section 4. par. D of the aforementioned law which provides that the Act shall not apply to the personal information processed for journalistic, artistic, literary or research purposes.

(7) Alumni, Donors, and Donee

- 7.1. Alumni relations, including:
 - 7.1.1. Maintaining alumni databases for linkage and job placement;
 - 7.1.2. Tracking alumni career paths and achievements.
- 7.2. Donation management, including:
 - 7.2.1. Complying with tax and anti-money laundering requirements;
 - 7.2.2. Recording donation sources and uses to ensure transparency.

(8) Contract Counterparties, Partners, Subcontractors, Outsourcers, Licensors, Licensees, Lessors, Lessees, Vendors, Purchasers, and Customers

- 8.1. Enforcing JHCSC's rights and obligations under law, contract, and public policy.
- 8.2. Meeting the intentions and goals of JHCSC in its partnerships and agreements.

(9) Other persons with a juridical link to JHCSC

- 9.1. Any applicable purposes above, as relevant to their association with JHCSC.
- 9.2. Unit-specific purposes aligned with the functions of similar bodies.

V. PROCESSING AND RETENTION OF PERSONAL DATA AT JHCSC

J.H. Cerilles State College (JHCSC) processes and retains Personal Data as required for its purposes in compliance with:

- (1) The Data Privacy Act of 2012, its Implementing Rules, and relevant guidelines from the National Privacy Commission;
- (2) The National Archives of the Philippines Act of 2007, its Implementing Rules, and applicable issuances from the National Archives of the Philippines;
- (3) Policies, procedures, and regulations established by JHCSC and its governing bodies;
- (4) Research protocols and ethical standards adopted by J.H. Cerilles State College; and
- (5) Executive Order No. 2, series of 2016 regarding Freedom of Information, along with any related executive orders issued thereafter.
- (6) Section 11. par. e of Data Privacy Act of 2012 "Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law".

In the absence of specific retention rules, Personal Data shall be stored by a JHCSC unit following the practices of government agencies with similar responsibilities.

VI. STORAGE AND TRANSMISSION OF PERSONAL DATA AT JHCSC

Personal Data at J.H. Cerilles State College (JHCSC) are stored in storage systems designed to protect the confidentiality, integrity, and availability of the data. These storage systems may include:

- (1) Electronic Databases: Personal Data are stored in encrypted digital databases that are accessible only to authorized personnel.
- (2) Physical Records: Where necessary, personal information may also be maintained in secure physical files, which are kept in locked cabinets or controlled access areas.
- (3) JHCSC may utilize third-party cloud services for data storage, ensuring that these services comply with relevant data protection regulations.

VI.I. Transmission of Personal Data

Personal Data are transmitted securely using the following methods:

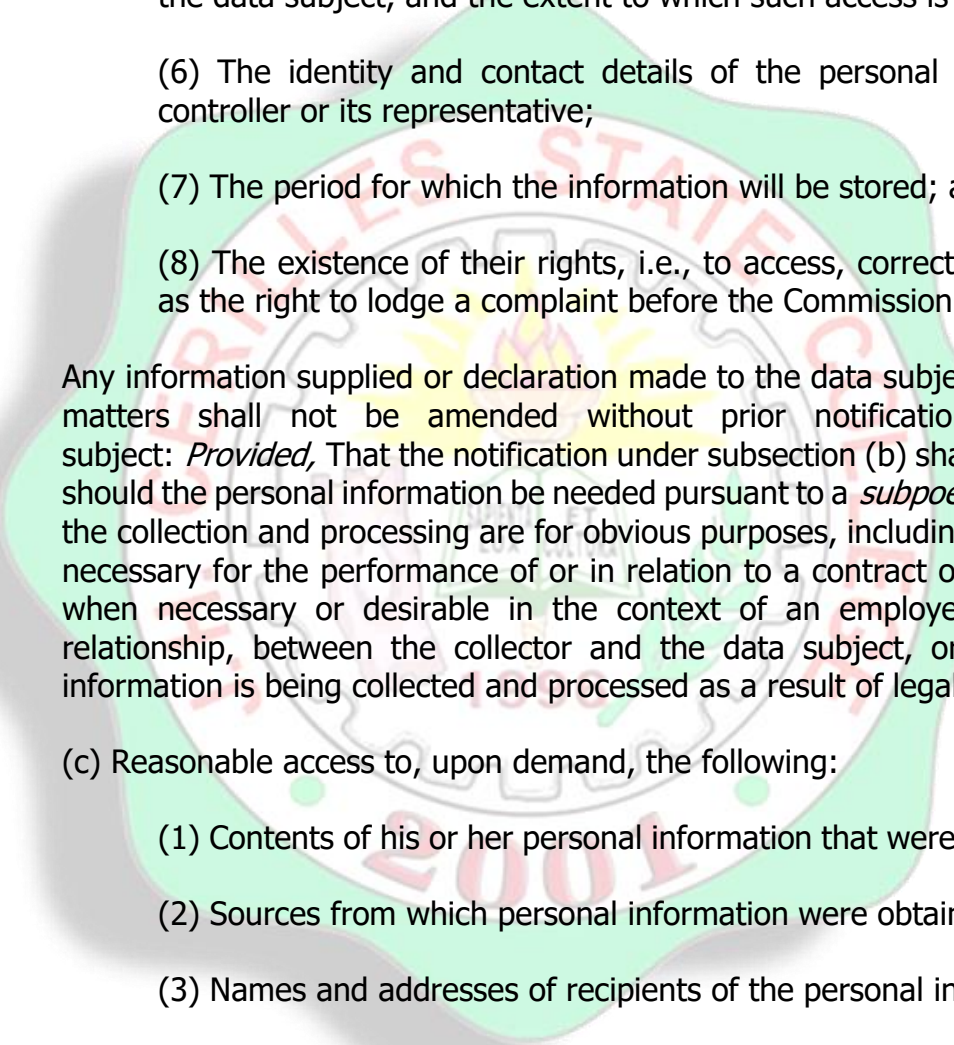
- (1) Secure Email: When sharing Personal Data via email, secure email protocols (such as encryption) are utilized to ensure data protection during transmission.
- (2) Secure File Transfer Protocols: Data transfers may be conducted using secure file transfer protocols to safeguard the integrity of the information.
- (3) Internal Networks: Personal Data are transmitted over secured internal networks that restrict access to authorized users only.
- (4) Third-Party Agreements: When sharing Personal Data with external parties, JHCSC ensures that agreements are in place to maintain confidentiality and compliance with data protection laws.

VII. RIGHT OF JHCSC COMMUNITY

Members of the J.H. Cerilles State College (JHCSC) community have the following rights regarding their Personal Data, following the Data Privacy Act of 2012, Section 16. Rights of the Data Subject, vis a vis:

SEC. 16. *Rights of the Data Subject.* – The data subject is entitled to:

- (a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;
- (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
 - (1) Description of the personal information to be entered into the system;

- 
- (2) Purposes for which they are being or are to be processed;
 - (3) Scope and method of the personal information processing;
 - (4) The recipients or classes of recipients to whom they are or may be disclosed;
 - (5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
 - (6) The identity and contact details of the personal information controller or its representative;
 - (7) The period for which the information will be stored; and
 - (8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: *Provided*, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a *subpoena* or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

(c) Reasonable access to, upon demand, the following:

- (1) Contents of his or her personal information that were processed;
- (2) Sources from which personal information were obtained;
- (3) Names and addresses of recipients of the personal information;
- (4) Manner by which such data were processed;
- (5) Reasons for the disclosure of the personal information to recipients;
- (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name or identity and address of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided*, That the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

VIII. RESPONSIBILITIES OF JHCSC COMMUNITY:

- (1)** Respect the data privacy rights of others;
- (2)** Report any suspected Security Incident or Personal Data Breach to JHCSC through the contact information in this Policy's Section on "The JHCSC Data Protection Officer";
- (3)** Provide the J.H. Cerilles State College (JHCSC) with true and accurate Personal Data and other information. Before submitting Personal Data of other people to JHCSC, obtain the consent of such people;
- (4)** Not disclose to any unauthorized party any non-public confidential, sensitive or personal information obtained or learned in confidence from JHCSC; and
- (5)** Abide by the policies, guidelines and rules of the JHCSC System and JHCSC on data privacy, information security, records management, research and

ethical conduct. From time to time check for and comply with updates on these policies, guidelines and rules. JHCSC policies on data privacy are at <https://jhcsc.edu.ph/>. For students, the JHCSC System's JHCSC Privacy Notice for Students can be found in this link.

IX. CONFIDENTIALITY NOTICE TEMPLATE:

All documents containing confidential information should follow this format:

CONFIDENTIALITY NOTICE: *The contents of this document and any accompanying materials are intended solely for the designated recipient(s) and may contain confidential and/or privileged information protected by law. Unauthorized access, disclosure, copying, or distribution of this document and its contents is strictly prohibited.*

X. EFFECTIVITY OF THIS POLICY:

The JHCSC Data Protection Officer may issue policies, guidelines, and rules consistent with this Policy to support its implementation.

If any law or regulation referenced in this Policy is amended or superseded, it is understood that this Policy will be interpreted in light of the updated or replacement law or regulation, ensuring that individuals' rights against retroactive application of laws are respected.

If any provision of this Policy is declared null and void, the remaining unaffected provisions shall continue to be in full force and effect.

PRIVACY POLICY FOR STUDENTS, PARENTS AND GUARDIANS

RATIONALE

This policy guides JHCSC students, parents, and guardians whose personal information, sensitive information, and privileged information are processed by the College.

As part of its mission and commitment to quality education, JHCSC aims to uphold leadership in higher education and community development, which is consistent with its mandate as a public institution.

This policy seeks to inform JHCSC students, parents, and guardians on how the College collects and processes Personal Data.

JHCSC is dedicated to fostering a culture of privacy by following the regulations and measures outlined in the Data Privacy Act of 2012, alongside the directives of the JHCSC Data Protection Office.

I. DEFINITION OF TERMS:

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

- 1.1. Data Privacy Act (DPA) refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012.
- 1.2. Data Processing System refers to either a computerized system or physical records that store, process, or transmit personal or sensitive information managed by any JHCSC unit or office.
- 1.3. Data Subject refers to an individual whose personal information is processed. For this Policy, "Data Subject" pertains to JHCSC students, parents, and guardians.
- 1.4. IRR refers to the Implementing Rules and Regulations of Republic Act No. 10173, also known as the Data Privacy Act of 2012.
- 1.5. Parents or Guardians refers to individuals or heads of institutions/family or foster homes who have custody of a student.
- 1.6. Personal Data includes all types of personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012 and its Implementing Rules and Regulations.
- 1.7. Personal Data Breach refers to a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized

disclosure, or access to personal data that has been transmitted, stored, or otherwise processed.

- 1.8. Privacy Risk refers to the potential loss of control over personal information if a threat exploits a vulnerability.
- 1.9. Processing involves any operation or set of operations performed upon personal information, including but not limited to collection, recording, organization, storage, updating, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.
- 1.10. Security Incident refers to any event that affects or could affect data protection or that may compromise the availability, integrity, and confidentiality of personal data. This includes incidents that might result in a personal data breach if not for the safeguards in place.
- 1.11. Student refers to individuals enrolled in or formally studying at JHCSC and who regularly attend classes.
- 1.12. Units and Offices refers to JHCSC's academic and administrative units and offices.

II. DATA COLLECTION AND PROTECTION OF PERSONAL DATA OF STUDENTS, PARENTS, AND GUARDIANS:

2.1. THE DATA LIFE CYCLE IN JHCSC

The data life cycle refers to the stages through which personal data passes, from the moment it is collected to its eventual disposal. At J.H. Cerilles State College (JHCSC), this life cycle is a systematic process that ensures all personal data is handled with the utmost care, security, and compliance with the Data Privacy Act of 2012. The College is committed to protecting the personal information of its stakeholders—students, parents, and guardians—at every stage of this life cycle.

Stages of the Data Life Cycle:

1. Collection

Personal data is gathered through various means, such as application forms, enrollment systems, and other official records. During this stage, JHCSC ensures transparency by informing stakeholders of the purpose for which their data is collected.

2. Processing

The data collected is processed for specific purposes, such as student enrollment, academic monitoring, and communication. This involves organizing, analyzing, and using the data in a lawful and secure manner.

3. *Storage*

Data is securely stored, whether in physical files or electronic databases. JHCSC employs advanced security measures to prevent unauthorized access, breaches, or loss of personal information.

4. *Usage*

Personal data is used strictly for its intended purposes, such as academic evaluations, administrative requirements, or other lawful activities in line with the College's operations.

5. *Sharing* and *Disclosure*

When necessary, personal data may be shared with authorized third parties, such as government agencies or accrediting bodies, but only under strict conditions to ensure data security and confidentiality.

6. *Retention*

Personal data is retained for as long as it is necessary to fulfill its purpose or comply with legal and regulatory requirements. JHCSC adheres to retention policies to determine the appropriate period for keeping records.

7. *Disposal*

Once the data is no longer needed, JHCSC ensures its secure and irreversible disposal to prevent misuse or unauthorized access.

By understanding and adhering to the stages of the data life cycle, JHCSC upholds its responsibility to protect personal data and foster trust among its stakeholders. Students, parents, and guardians should remain informed and mindful of these processes to better appreciate how their data is managed and safeguarded.

2.1.1. COLLECTION OF PERSONAL DATA

JHCSC collects Personal Data during the application for admission, registration, enrollment, and throughout the engagement of students, parents, and guardians with the College.

- 2.1.1.1. Personal details, such as name, age, color, race, ethnic background, origin, birthdate, gender, civil status, and affiliations
- 2.1.1.2. Contact information, such as address, email, mobile, and telephone numbers
- 2.1.1.3. Academic information, such as grades, course and academic standing
- 2.1.1.4. Medical information, including physical, psychiatric, and psychological records

Data is collected through various forms and documents, in compliance with relevant laws and policies, including the JHCSC Charter and the Data Privacy Act of 2012.

2.1.2. STORAGE AND TRANSMISSION OF DATA

Collected Personal Data is stored securely in physical and electronic “Data Processing Systems,” with security measures per National Privacy Commission Circular No. 17-01. Each academic unit and administrative office of JHCSC uses designated systems and secure locations to store data.

Transmission of data is carried out following JHCSC's prescribed procedures, and the College implements robust safety measures to prevent unauthorized access, disclosure, or data loss. Security protocols are aligned with JHCSC's Information Security and Physical and Organizational Security policies.

2.1.3. USE OF PERSONAL DATA

Authorized JHCSC staff and faculty access and use Personal Data for purposes consistent with the College's mandate under the JHCSC charter and other regulations. Specific purposes include:

2.1.3.1. ACADEMIC PURPOSES

- (1) Admissions and compliance with CHED Orders and Memoranda
- (2) Scholastic recognitions and awards
- (3) Processing and evaluating grades
- (4) Developing and implementing JHCSC Academic policies and regulations

2.1.3.2. EXTRA-CURRICULAR PURPOSES

- (1) Managing student organizations
- (2) Collaborating with external institutions
- (3) Conducting school activities, social programs, and guidance programs

2.1.3.3. MEDICAL PURPOSES

- (1) Providing medical, dental, psychiatric, and psychological support

- (2) Maintaining health records to better understand and respond to students' medical needs.

2.1.3.4. STUDENT ASSISTANCE PURPOSES

- (3) Offering legal, scholarship, financial, and dormitory aid
- (4) Providing tutoring, mentorship, or internship assistance
- (5) Assisting families during emergencies, calamities, or pandemics

2.1.3.5. STUDENT DISCIPLINARY PURPOSES

- (6) Investigating and addressing violations of College regulations
- (7) Imposing sanctions as per disciplinary policies
- (8) Complying with applicable laws and government orders

2.1.3.6. ADDITIONAL PURPOSES

- (1) Records and account management
- (2) Ensuring campus security and community welfare
- (3) Conducting JHCSC's institutional responsibilities, rights, and functions as a higher education institution and government instrumentality

2.1.4. RETENTION OF DATA

The retention of files or documents containing Personal Data, in both physical and electronic formats, shall adhere to the guidelines set by:

- 2.1.4.1. The Data Privacy Act of 2012, the National Archives of the Philippines Act of 2007, and their Implementing Rules and Regulations.
- 2.1.4.2. JHCSC policies, guidelines, and rules on data privacy, record-keeping, record monitoring, and management, including the JHCSC Data Classification and Records Management Policies, and research and ethical standards.
- 2.1.4.3. Relevant executive and regulatory issuances, such as those governing Freedom of Information.
- 2.1.4.4. Section 11. par. e of Data Privacy Act of 2012 "Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law".

2.1.5. DISPOSAL AND DESTRUCTION OF DATA

When it becomes necessary to dispose of or permanently delete records (including Personal Data), JHCSC ensures complete destruction by means such as shredding, burning, pulping, or other methods that prevent any reconstruction of the information contained therein.

2.2. DATA PRIVACY PRINCIPLES

Each stage of the data life cycle shall strictly adhere to the core data privacy principles of transparency, legitimate purpose, and proportionality.

2.2.1. TRANSPARENCY

Data Subjects should be fully informed about the nature, purpose, and scope of how their personal data is processed. This includes understanding the associated risks, available safeguards, the identity of the personal information controller (such as JHCSC and its relevant academic and administrative units), as well as their rights as Data Subjects and the ways to exercise these rights. Information regarding the data processing should be readily accessible and communicated in clear, simple language for ease of understanding.

To uphold this transparency, JHCSC will provide a comprehensive privacy policy and a privacy notice, both accessible on the JHCSC Data Protection Office website. This ensures that Students, Parents, and Guardians have access to necessary information regarding their data privacy rights and protections.

2.2.2. LEGITIMATE PURPOSE

J.H. Cerilles State College (JHCSC), as an established institution of higher learning, is committed to fulfilling its mandate as outlined by the relevant laws and regulations. In accordance with its mission to contribute to the development of future leaders through quality education, JHCSC processes the personal data of Students, Parents, and Guardians solely to support its educational, administrative, and institutional objectives.

The collection and processing of personal data are carried out in compliance with the following legal frameworks, among others:

- (1) The Data Privacy Act of 2012;
- (2) The National Archives of the Philippines Act of 2007, along with its Implementing Rules and Regulations;
- (3) JHCSC's Privacy Policy and Records Management Policy;
- (4) Policies, guidelines, and regulations issued by JHCSC and applicable governmental bodies;
- (5) Executive Order No. 2, Series of 2016 on Freedom of Information and subsequent related directives; and
- (6) Other relevant legal mandates or amendments to these regulations.

2.2.3. PROPORTIONALITY

The processing of personal data at JH Cerilles State College (JHCSC) shall adhere to the principles of adequacy, relevance, suitability, necessity, and shall not exceed what is required to achieve the legitimate purposes established by the institution.

In alignment with these privacy principles, it is crucial that all stages of the data life cycle are managed with diligence. JHCSC's units and offices are committed to implementing necessary measures to safeguard the personal data of Students, Parents, and Guardians, ensuring that such data is handled responsibly and in proportion to its intended use.

2.3. SECURITY MEASURES

J.H. Cerilles State College (JHCSC) is responsible for maintaining and safeguarding the personal information under its care. The College designates individuals who oversee the collection, safekeeping, and adherence to JHCSC's data privacy policies.

The security measures are designed to ensure the availability, integrity, and confidentiality of personal data, protecting it against both natural threats, such as accidental loss or destruction, and human threats, including unauthorized access, fraudulent misuse, unlawful destruction, alteration, and contamination.

2.4. ORGANIZATIONAL SECURITY MEASURES

- 2.4.1. JH Cerilles State College (JHCSC) staff and faculty participate in regular training sessions provided by the JHCSC Data Protection Office.
- 2.4.2. Each academic unit and administrative office is represented by a Privacy Focal Person (PFP), who supports the JHCSC Data Protection Office and implements privacy and security initiatives specific to their unit or office.
- 2.4.3. The PFPs will identify privacy risks by conducting privacy impact assessments and proposing measures to mitigate those risks.

2.5. PHYSICAL SECURITY MEASURES

- 2.5.1. The personal data collected are maintained in both physical and electronic formats. All records must be stored in secure locations, including locked filing cabinets.
- 2.5.2. Access to storage locations, facilities, and devices containing personal data is restricted to authorized JH Cerilles State College (JHCSC) staff and faculty. Other personnel may be granted access only with the approval of the Data Protection Officer, based on requests from the head and the Privacy Focal Person (PFP) of the relevant JHCSC unit or office.
- 2.5.3. JHCSC staff and faculty must take precautions to protect all printed and electronic personal data. Laptops and desktop computers should be locked when not in use, and passwords or passphrases must not be written down or made accessible to others.

2.6. TECHNICAL SECURITY MEASURES

The Technical Security Measures outline the methods used for authentication and safeguarding against the theft of sensitive data and information. These measures ensure that only verified user applications can access and read data. The following technical security measures are designed to assist JH Cerilles State College (JHCSC) staff and faculty in mitigating risks and preventing security breaches:

- 2.6.1. Communication among JHCSC students, faculty, and staff should utilize JHCSC email accounts for standard encryption, professionalism, and institutional identity.
- 2.6.2. Use of passphrases—longer phrases or combinations of words—rather than single words as passwords to enhance security.
- 2.6.3. Regular backups of personal data should be conducted. The frequency of backups should increase with the importance of the data and the rate of changes made to it.

- 2.6.4. Any person, whether affiliated with JHCSC or not, must report a Security Incident or Personal Data Breach within two (2) hours of discovery. This can be done by emailing the subject line "Incident/Breach – Name of the Unit" to dpo@jhcsc.edu.ph or by calling both the JHCSC Data Protection Officer and the Privacy Focal Person responsible for the affected unit, in accordance with the Security Incident Management Policy.
- 2.6.5. The JHCSC Data Protection Office provides a guide to help protect the college's information and information systems, ensuring their confidentiality, integrity, and availability, as outlined in the Information Security Policy.

III. ACCESS TO PERSONAL DATA

- (1) Only authorized JH Cerilles State College (JHCSC) staff and faculty members are permitted to access personal information. The specific authorized personnel may vary by unit within JHCSC.
- (2) Contractors, consultants, and service providers may also access personal information; however, their access will be governed by stringent procedures outlined in formal contracts. These contracts must comply with the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), and all applicable issuances from the National Privacy Commission (NPC) and JHCSC. The terms of these contracts and the commitments made must be subject to review and audit to ensure compliance.
- (3) JHCSC may disclose a data subject's personal information to third parties in connection with the purposes for which it was collected, as consented to by the data subjects, or as required or permitted by law.
- (4) Authorized users of personal information must adhere to the JHCSC Policy on Acceptable Use of Information Assets. This policy can be found at <https://jhcsc.edu.ph>
- (5) For authorized users accessing personal information online, authentication of their identity will be conducted via a secure encrypted link, and they must utilize the security measures prescribed in this policy, as well as any other relevant security policies of the State College.

3.1. PERSONAL DATA CAN BE SHARED TO OTHER ORGANIZATION OR INSTITUTION.

- 3.1.1. The personal data collected are maintained in both physical and electronic formats. All records must be stored in secure locations, including locked filing cabinets.
- 3.1.2. Personal data may also be shared through a process known as anonymization. Data is considered anonymized

when there are no possible means to identify the data subject, meaning that JHCSC's offices, units, or any other entities cannot single out an individual in a data set. This includes being unable to connect two records within a data set (or between two separate data sets) or identify any information in such a dataset.

- 3.1.3. It is important to note that shared anonymized data cannot be used, directly or indirectly, to identify a person.

3.2. PERSONAL DATA CAN BE ACCESS BY THE STUDENTS, PARENTS AND GUARDIANS.

The personal information of Students, Parents, and Guardians at JH Cerilles State College (JHCSC) will be made available to them upon request, in accordance with the Data Privacy Act of 2012 and the guidelines issued by the JHCSC Data Protection Office.

- 3.2.1. The academic units and administrative offices of JHCSC will establish guidelines for Students, Parents, and Guardians to access and request updates to their personal information. These guidelines will include:

- **Access Request Form:** An access request form will be provided to the Data Subject upon their request.
- **Assessment of Validity:** JHCSC units and offices will assess and evaluate the validity of the request.
- **Access Provision:** Access to personal information will be granted to the Data Subject in accordance with JHCSC's policies and regulations.

3.3. ACCURACY AND UP-TO-DATE PERSONAL DATA

- 3.3.1. JH Cerilles State College (JHCSC) is committed to ensuring that personal data are, in accordance with the Data Privacy Act (DPA), "accurate, relevant, and, where necessary, kept up to date for the purposes for which it is to be used." This commitment is crucial, as any inaccuracies or incomplete data can lead to incorrect decisions and interpretations based on the collected information.
- 3.3.2. The DPA further mandates that "inaccurate or incomplete data must be rectified, supplemented, destroyed, or their further processing restricted." This means that JHCSC will

take necessary actions to correct any inaccuracies promptly.

- 3.3.3. Moreover, when updating contact information, careful attention must be given to mitigate risks associated with inadvertently sending personal and/or sensitive personal information to unintended recipients. JHCSC will implement strict procedures to verify the identity of individuals requesting updates to their information to ensure data privacy and security.

IV. CONSENT

Generally, obtaining a data subject's consent is a prerequisite for the lawful processing of their personal data. However, this requirement is not absolute, as the State College may process a faculty member's personal data without their consent under the following conditions:

4.1. CONTRACT FULFILLMENT

- 4.1.1. The processing of personal information is necessary to fulfill a contract with the data subject or to take steps requested by the data subject prior to entering into a contract.

4.2. LEGAL OBLIGATION

- 4.2.1. The processing is necessary for compliance with a legal obligation to which JHCSC, as the personal information controller, is subject.

4.3. VITAL INTERESTS

- 4.3.1. The processing is necessary to protect the vitally important interests of the data subject, including their life and health.

4.4. NATIONAL EMERGENCY AND PUBLIC OFFICER

- 4.4.1. The processing is necessary in response to a national emergency, to comply with public order and safety requirements, or to fulfill functions of public authority, which includes processing personal data to meet institutional mandates.

4.5. LEGITIMATE INTERESTS

- 4.5.1. The processing is necessary for the legitimate interests pursued by JHCSC or a third party to whom the data is disclosed, except when such interests are overridden by the fundamental rights and freedoms of the data subject that require protection under the Philippine Constitution.

V. RIGHTS OF DATA SUBJECT

The access of personal data is one of the rights of the Data Subjects. In addition to the right to access, Students, Parents, and Guardians have the following rights that must be observed by J.H. Cerilles State College:

5.1. RIGHT TO BE INFORMED

- 5.1.1. This should answer the questions like, "Why you collect and what will you do to my personal data?", "How will you process my personal data?", "Who can I contact for questions?", "How will you protect my personal data?", and "How can I exercise my rights?"
- 5.1.2. Data Subjects have the right to be informed about the collection and processing of their personal data, including the purpose of such processing and the identities of the individuals or entities involved.

5.2. RIGHT TO ACCESS

- 5.2.1. Data Subjects have the right to demand reasonable access to their personal information. It should be given in a clear and understandable format.

5.3. RIGHT TO OBJECT, AND RIGHT TO CORRECT OR RECTIFY

- 5.3.1. Every Student, Parent and Guardian has the right to dispute the accuracy in their personal data and have the same rectified or corrected.

5.4. RIGHT TO ERASURE OR BLOCKING

- 5.4.1. These rights of erasure and blocking do not apply to Personal Data, documents, records and accounts which are part of JHCSC public records as an instrumentality of the government. It may be exercised if there is a substantial proof that the processing of Personal Data is unlawful.

5.5. RIGHT TO DATA PORTABILITY

- 5.5.1. Where his or her Personal Data is processed by electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain from JHCSC a copy of such data in an electronic or structured format that is commonly used and allows for further use by the Data Subject.

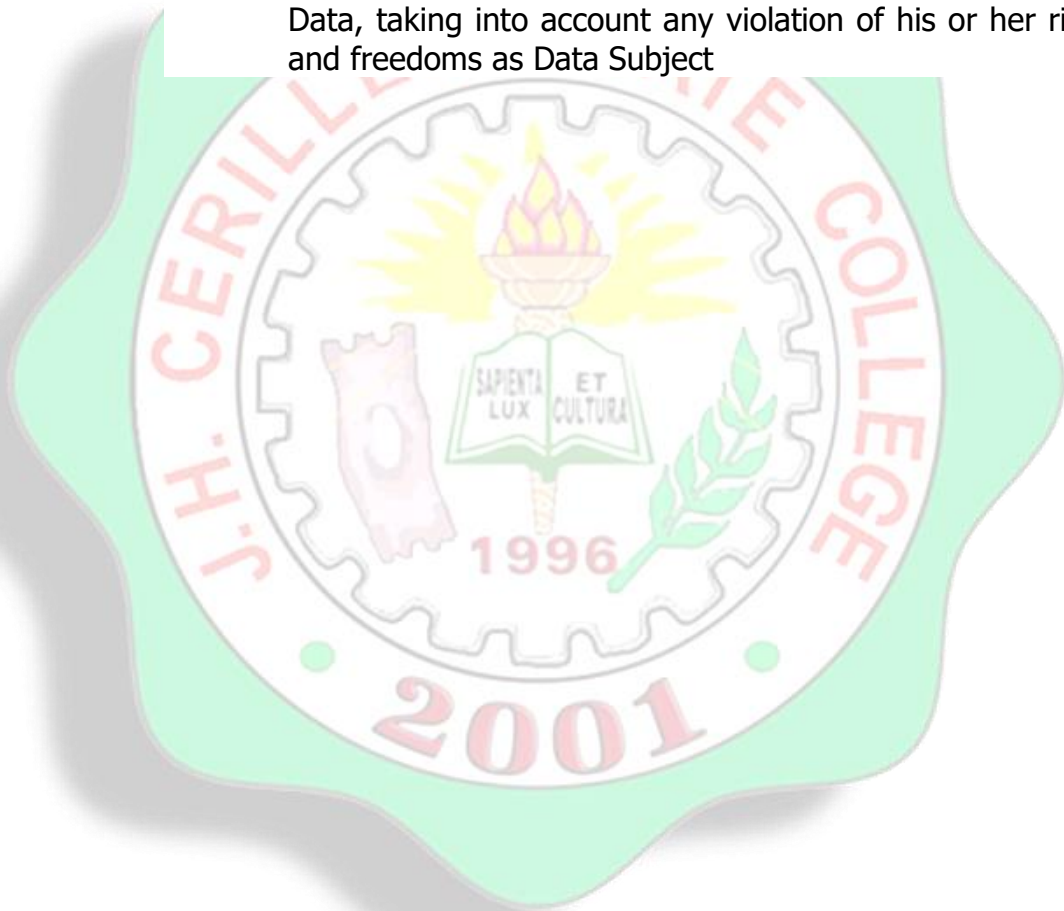
5.6. RIGHT TO FILE A COMPLAINT

- 5.6.1. The Data Subject have a right to complain when they see that there is a violation of his or her rights as Data Subject and for any injury suffered as a result of the processing of his or her Personal Data.

- 5.6.2. The Data Subject must write to the Director of the Office or Dean of the College and an internal investigation will proceed. Should the complaint remain unresolved, the complaint may be forwarded to the JHCSC Data Protection Office addressed to the Data Protection Officer for further investigation and resolution. The result thereof may be forwarded to the Office of the President for information and reference.

5.7. RIGHT TO DAMAGE

- 5.7.1. The Data Subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data, taking into account any violation of his or her rights and freedoms as Data Subject



PRIVACY POLICY FOR STAFF

RATIONALE

The Staff plays a crucial role in fulfilling the State College's mandate. In executing this mandate, it is essential for the State College to prioritize the protection of the personal information of its Staff. This Derivative Policy aims to outline and discuss the processes involved in managing the Staff's personal information in compliance with the Data Privacy Act of 2012. The policy will ensure that all staff members are aware of their rights regarding their personal data and that the State College implements appropriate measures to safeguard their information throughout its lifecycle, from collection to disposal. By adhering to these guidelines, the State College commits to fostering a secure environment that respects the privacy and confidentiality of its Staff's personal information.

I. DEFINITION OF TERMS

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

- 1.1. Data Privacy Act (DPA)** refers to Republic Act No. 10173 or the Data Privacy Act of 2012;
- 1.2. Data Processing System** refers to either a computerized system or physical records that store, process, or transmit personal information or sensitive personal information owned or managed by a JHCSC unit or office;
- 1.3. Data Subject** refers to an individual whose personal information is processed. For the purposes of this Policy, the term Data Subject shall refer to the Staff, Research, Extension, and Professional Staff (REPS), and Contractuals;
- 1.4. IRR** refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
- 1.5. NPC** refers to the National Privacy Commission of the Philippines as created by the Data Privacy Act of 2012;
- 1.6. Personal Data** refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012;
- 1.7. Privacy Risk** refers to the potential loss of control over personal information when a threat exploits a vulnerability;
- 1.8. Processing** refers to any operation or set of operations performed upon personal information, including but not limited to collection, recording, organization, storage, updating or modification, retrieval, consultation,

- use, consolidation, blocking, erasure, or destruction of data;
- 1.9. Staff** refers to the State College Staff, including Research, Extension, and Professional Staff (REPS), JHCSC contractual personnel, non-JHCSC contractual personnel, and retired REPS and Administrative Staff;
- 1.10. Units and Offices** refers to JHCSC academic units and administrative offices.

II. CARDINAL PRINCIPLES OF DATA PRIVACY IN RELATION TO THE PROCESSING OF THE STAFF'S PERSONAL DATA

2.1. TRANSPARENCY

The JHCSC shall process the personal information of its staff only after ensuring that they are informed of the identification of the office or unit collecting their personal data, as well as the nature, purpose, and extent of its processing.

2.2. LEGITIMATE PURPOSE

The JHCSC shall process its data subjects' personal information in accordance with its declared and specified purpose only. Furthermore, its processing must not be contrary to law, morals, public policy, and pertinent issuances of this Institution.

The JHCSC processes personal data on the following grounds, to wit:

In fulfilling its obligations, exercising its rights, and conducting its related functions, JHCSC processes personal information for the following purposes:

- 2.2.1.** As a government instrumentality and higher education institution;
- 2.2.2.** For purposes that benefit the staff, as determined by the State College;
- 2.2.3.** To assess the provision or extension of assistance, housing, medical, or other benefits for staff and their families;
- 2.2.4.** To evaluate staff for promotions, transfers, benefits, salary increases, step increases, or rank adjustments;
- 2.2.5.** For the specific needs of JHCSC units, ensuring the conduct of customary and foreseeable activities;

- 2.2.6.** For managing and administering its internal and external operations as an academic and research institution, government body, and juridical an entity with its own rights and interests.

Corollary to that, the State College processes the collected personal data in accordance with the following laws, *viz*:

- (1) The Data Privacy Act of 2012;
- (2) The National Archives of the Philippines Act of 2007, including its Implementing Rules and Regulations, and other related issuances;
- (3) Republic Act No. 6713, Code of Conduct and Ethical Standards for Public Officials and Employees, which mandates that government employees must be accountable to the public and serve with responsibility, integrity, loyalty, and efficiency;
- (4) The JHCSC Privacy Manual; a. The JHCSC Records Management Policy; b. Policies, guidelines, and rules of JHCSC; c. Executive Order No. 2, series of 2016, or the Freedom of Information and its related issuances; and d. Other applicable laws or regulations that amend or replace the aforementioned

2.3. PROPORTIONALITY

JHCSC shall consistently adhere to the principle of data minimization, ensuring that it only processes personal data that are accurate, relevant, and necessary for the specified purpose(s). Additionally, JHCSC will refrain from processing personal data if the intended purposes of such processing can be reasonably achieved through other means.

III. PROCESSING OF PERSONAL DATA OF STAFF

The processing of personal data at JHCSC should be carried out only with the staff's knowledge and consent. However, JHCSC must ensure that it collects only the personal information necessary for its stated purposes and that the collection is conducted fairly and legally.

3.1. COLLECTION OF DATA

The collection of staff's personal data at J.H. Cerilles State College may be conducted through various data-gathering forms, including but not limited to written records (e.g., Personal Data Sheet) and photographic and video images.

Collected personal data may include any of the following:

- (1) Personal Details: (e.g., name, date of birth, sex, civil status)
- (2) Contact Information: (e.g., mobile number, email address, home address)
- (3) Academic Information: (e.g., educational background, scholastic records)
- (4) Employment Information: (e.g., Tax Identification Number (TIN), Philhealth ID Number, GSIS Membership, employee number)
- (5) Applicant Information: (e.g., former employment history, affiliations)
- (6) Medical Information: (e.g., physical examination, psychiatric evaluation, and drug test results)
- (7) Photographs or Videos: (e.g., for the official documentation of College activities or events)

3.2. USE OF PERSONAL DATA

The use of the staff's personal data at JHCSC shall always align with the State College mandate. Specifically, the use of personal data may include the following:

- (1) Academic, research, extra-curricular, student welfare, and disciplinary purposes.
- (2) Administrative disciplinary purposes.
- (3) Supervision of academic and research endeavors.
- (4) Management of human resources and supervision of work conduct.
- (5) Employee application processing and identity verification.
- (6) Documentation and record-keeping.
- (7) Customer, client, patient, or community service initiatives.
- (8) Contractual and financial purposes.
- (9) Corporate governance and housekeeping.
- (10) Regulatory and audit compliance
- (11) Performance evaluation.
- (12) Documentation of the JHCSC's official activities and events.
- (13) Recognition and awards.
- (14) Identification of the necessity and legality of the purposes prior to or at the time personal information is collected, used, and disclosed.

(15) Other similar purposes that align with the JHCSC mandate.

3.3. STORAGE, RETENTION, DISPOSAL AND DESTRUCTION OF PERSONAL DATA

JHCSC shall ensure that all personal data it collects and uses are stored in secure facilities to prevent unauthorized access or use. The State College will implement necessary physical, organizational, and technical security measures to maintain the confidentiality, availability, and integrity of the stored personal data.

The retention of staff personal data will be limited to the duration necessary to comply with applicable laws, rules, and regulations, including National Archives' Circulars and JHCSC's Records Management Policy.

When the time for retention has expired, personal data will be disposed of and destroyed in a manner that ensures no part of the data is exposed, rendering its reconstitution impossible.

3.4. ACCESS

JHCSC shall ensure that only authorized personnel have access to the personal data of its staff. Access will be strictly limited to what is necessary for the fulfillment of their respective duties related to the processing of that personal data. Additionally, access to personal data will adhere to the JHCSC Data Classification Policy, ensuring compliance with established guidelines for data protection and privacy.

3.5. DISCLOSURE

JHCSC may send text messages or emails to staff for purposes related to work, operations, health, emergencies, and community matters. Online meetings may also be utilized to communicate and discuss work-related issues, especially in situations involving work-from-home arrangements.

This arrangement is based on the assumption that staff and personnel have consented to JHCSC gathering their contact information for the purpose of facilitating communication necessary to fulfill work assignments. Compliance with the State College data privacy, security, and confidentiality policies is essential when using text messaging and email platforms.

Only authorized personnel at JHCSC may disclose or transfer personal data, both within the State College and to external entities, provided that such actions remain consistent with the fundamental principles of data privacy.

IV. CONSENT

Generally, a data subject's consent is a prerequisite for the lawful processing of their personal data. However, this requirement is not absolute, and under the following conditions, JHCSC may process a staff member's personal data without obtaining consent:

- (1) The processing of personal information is necessary and related to the fulfillment of a contract with the data subject or to take steps at the request of the data subject prior to entering into a contract.
- (2) The processing is necessary for compliance with a legal obligation to which JHCSC, as the personal information controller, is subject.
- (3) The processing is necessary to protect vitally important interests of the data subject, including life and health.
- (4) The processing is necessary to respond to a national emergency, to comply with public order and safety requirements, or to fulfill functions of public authority that involve processing personal data in order to carry out the State College mandate.
- (5) The processing is necessary for the legitimate interests pursued by JHCSC or by a third party to whom the data is disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject that require protection under Philippine law.

V. SECURITY MEASURES

5.1. ORGANIZATIONAL SECURITY MEASURES

JHCSC shall continuously develop and apply appropriate organizational security measures to ensure the confidentiality, integrity, and availability of its staff's personal data. These measures include, but are not limited to, the following:

- (1) JHCSC Privacy Manual
- (2) JHCSC Data Classification Policy
- (3) Remote Work Privacy Guidelines
- (4) Data Protection in Work Processes
- (5) JHCSC Message and Communications Policy
- (6) JHCSC Email Policy
- (7) Other pertinent State College issuances

5.2. PHYSICAL SECURITY MEASURES

JHCSC shall ensure that the physical storage of its staff's personal data is always secured. Access to these storage facilities shall be limited only to authorized personnel.

Furthermore, JHCSC shall ensure that in the course of processing staff's personal data, the physical security measures prescribed by the JHCSC Privacy Manual are observed.

7.3. TECHNICAL SECURITY MEASURES

JHCSC shall apply the appropriate technical security measures to ensure that its staff's personal data remain confidential, available, and unaltered at all times. It shall adopt the necessary provisions on the Technical Security Measures in the JHCSC Data Privacy Manual and the National Privacy Commission's Circular on the Security of Personal Data in Government Agencies.

VI. RIGHTS OF DATA SUBJECT

5.1. RIGHT TO BE INFORMED

Every staff member has the right to be informed about the purpose of collecting, using, disclosing, and processing their personal data. This encompasses how the data will be processed and the offices or units responsible for handling it.

5.2. RIGHT TO ACCESS

Every staff member has the right, in accordance with relevant laws and JHCSC regulations, to reasonable access to their personal data processed by the College.

5.3. RIGHT TO OBJECT AND RIGHT TO CORRECT OR RECTIFY

Every staff member has the right to challenge the accuracy of their personal data and to have it rectified or corrected.

5.4. RIGHT TO ERASURE OR BLOCKING

The rights to erasure and blocking do not apply to personal data, documents, records, and accounts that are part of JHCSC's public records as an instrumentality of the government or as a State College. However, these rights may be exercised if there is substantial proof that the processing of personal data is unlawful.

5.5. RIGHT OF DATA PORTABILITY

Every staff member has the right, subject to relevant laws and JHCSC rules and regulations, to request a copy of their personal data in a commonly used format that allows for further use.

5.6. RIGHT TO FILE A COMPLAINT AND RIGHT TO DAMAGES

Every staff member has the right to file a complaint if their personal information has been misused, maliciously or improperly disclosed, or if any of the aforementioned rights have been violated. They also have the right to be indemnified for any damages suffered due to such violations.

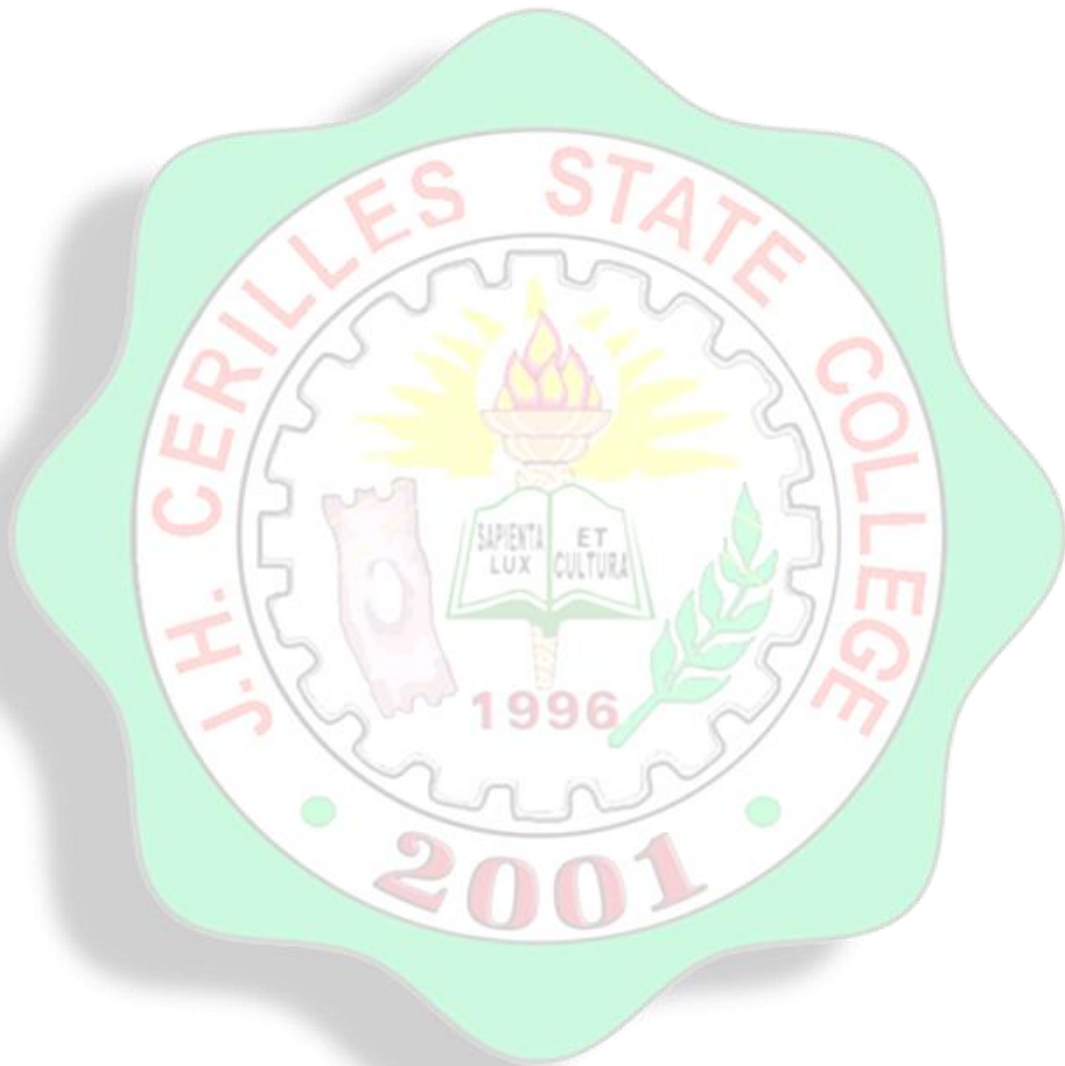
VII. GROUP CHATS

Group chats among Staff members are commonly used to facilitate communication and collaboration. However, these platforms may also involve the sharing of personal data or sensitive information, requiring adherence to data privacy principles. JHCSC establishes the following policy for group chats among faculty:

- 7.1. Group chats should be used exclusively for academic, administrative, or professional purposes. Staff members must avoid sharing personal opinions or unrelated content that could compromise professionalism.
- 7.2. Personal information of students, colleagues, or third parties must not be disclosed in group chats unless it is strictly necessary for legitimate purposes and authorized by the relevant parties.
- 7.3. Sensitive information, such as grades or disciplinary actions, must only be shared through secured and approved channels, not through group chats
- 7.4. Only authorized staff members may join group chats. Membership lists should be regularly reviewed to ensure only current and relevant participants remain in the group.
- 7.5. Staff members should use official or institution-approved communication platforms that comply with data privacy standards.
- 7.6. Chats that involve institutional matters or official decisions must be archived or recorded as necessary, following data retention policies.

Informal or personal group chats should not contain institutional data.

- 7.7 Any suspected breach of confidentiality or inappropriate use of the group chat must be reported immediately to the designated Data Privacy Officer for investigation.



PRIVACY POLICY FOR FACULTY

RATIONALE

The faculty members of J.H. Cerilles State College play a crucial role in fulfilling the institution's mandate as a premier educational establishment. In carrying out this mandate, it is imperative for the College to ensure the protection of the personal information of its faculty members.

This Derivative Policy is designed to outline and address the procedures by which J.H. Cerilles State College manages the processing of faculty personal information, in compliance with the Data Privacy Act of 2012.

(1) DEFINITION OF TERMS

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

- 1.1. Data Privacy Act (DPA)** refers to Republic Act No. 10173 or the Data Privacy Act of 2012.
- 1.2. Data Processing System** refers to either a computerized system or physical records that store, process, or transmit personal information or sensitive personal information owned or managed by J.H. Cerilles State College.
- 1.3. Data Subject** refers to an individual whose personal information is processed. For the purposes of this Policy, the term Data Subject shall refer to the members of the faculty.
- 1.4. Faculty** refers to the teaching staff of each academic unit, comprising both regular and non-regular faculty members.
- 1.5. IRR** refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012.
- 1.6. NPC** refers to the National Privacy Commission of the Philippines, as created by the Data Privacy Act of 2012.
- 1.7. Personal Data** refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012.
- 1.8. Privacy Risk** refers to the potential loss of control over personal information when a threat exploits vulnerability.
- 1.9. Processing** refers to any operation or set of operations performed upon personal information, including but not limited to the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.

1.10. Units and Offices refers to the academic units and administrative offices of J.H. Cerilles State College.

(2) PRINCIPLES OF DATA PRIVACY IN RELATION TO THE PROCESSING OF THE FACULTY'S PERSONAL DATA

2.1. TRANSPARENCY

J.H. Cerilles State College shall process the personal information of its faculty only after ensuring that they are informed of the identification of the office or unit collecting their personal data, as well as the nature, purpose, and extent of its processing.

2.2. LEGITIMATE PURPOSE

J.H. Cerilles State College shall process its data subjects' personal information only in accordance with its declared and specified purposes. Furthermore, such processing must not be contrary to law, morals, public policy, and relevant issuances of the College.

J.H. Cerilles State College processes personal data on the following grounds:

- 2.2.1.** In the performance of its obligations, exercising its rights, and conducting its associated functions as a:
 - (1) Government instrumentality
 - (2) Higher education institution
- 2.2.2.** In pursuance of its purpose and mandate under Republic Act No. 9500 and other relevant laws;
- 2.2.3.** In the conduct of all acts that are reasonably foreseeable and customarily performed by similar bodies;
- 2.2.4.** Making decisions and acting for the holistic welfare of its students, their parents and guardians, faculty, staff, researchers, alumni, and the broader J.H. Cerilles State College community;
- 2.2.5.** Managing and administering its internal and external affairs as an academic and research institution, government instrumentality, and juridical entity with its own rights and interests.

Corollary thereto, J.H. Cerilles State College processes the collected personal data in accordance with the following laws:

- (1) The Data Privacy Act of 2012
- (2) The National Archives of the Philippines Act of 2007, including its Implementing Rules and Regulations, and other issuances
- (3) The J.H. Cerilles State College Privacy Manual
- (4) The J.H. Cerilles State College Records Management Policy
- (5) Policies, guidelines, and rules of the J.H. Cerilles State College System
- (6) Relevant Executive Orders and issuances pertaining to freedom of information
- (7) Other laws or regulations related to, or which amend or repeal the foregoing.

2.3. PROPORTIONALITY

J.H. Cerilles State College shall constantly abide by the principle of data minimization, ensuring that it processes only personal data that are accurate, relevant, and necessary for the declared purpose(s).

Furthermore, the College will not process personal data if the purposes of the processing can be reasonably fulfilled by other means.

(3) PROCESSING OF PERSONAL DATA OF FACULTY

3.1. COLLECTION OF PERSONAL DATA

Collection of faculty's personal data at J.H. Cerilles State College may be conducted through various data-gathering forms, including but not limited to written records (e.g., Personal Data Sheet) and photographic and video images.

The collected personal data may include any of the following:

- (1) Personal Details: (e.g., name, date of birth, sex, civil status)
- (2) Contact Information: (e.g., mobile number, email address, home address)
- (3) Academic Information: (e.g., educational background, scholastic records)
- (4) Employment Information: (e.g., Tax Identification Number (TIN), Philhealth ID Number, GSIS Membership, employee number)
- (5) Applicant Information: (e.g., former employment history, affiliations)
- (6) Medical Information: (e.g., physical examination, psychiatric evaluation, and drug test results)
- (7) Photographs or Videos: (e.g., for the official documentation of College activities or events)

3.2. USE OF PERSONAL DATA

The use of the faculty's personal data at JHCSC shall always align with the State College mandate. Specifically, the use of personal data may include the following:

- (1) Academic, research, extra-curricular, student welfare, and disciplinary purposes.
- (2) Administrative disciplinary purposes.
- (3) Supervision of academic and research endeavors.
- (4) Management of human resources and supervision of work conduct.
- (5) Employee application processing and identity verification.
- (6) Documentation and record-keeping.
- (7) Customer, client, patient, or community service initiatives.
- (8) Contractual and financial purposes.
- (9) Corporate governance and housekeeping.
- (10)Regulatory and audit compliance
- (11)Performance evaluation.
- (12)Documentation of the JHCSC's official activities and events.
- (13)Recognition and awards.
- (14)Identification of the necessity and legality of the purposes prior to or at the time personal information is collected, used, and disclosed.
- (15)Other similar purposes that align with the JHCSC mandate.

3.3. STORAGE, RETENTION, DISPOSAL AND DESTRUCTION OF PERSONAL DATA

JHCSC shall ensure that all personal data it collects and uses are stored in secure facilities to prevent unauthorized access or use. The State College will implement necessary physical, organizational, and technical security measures to maintain the confidentiality, availability, and integrity of the stored personal data.

The retention of faculty personal data will be limited to the duration necessary to comply with applicable laws, rules, and regulations, including National Archives' Circulars and JHCSC's Records Management Policy.

When the time for retention has expired, personal data will be disposed of and destroyed in a manner that ensures no part of the data is exposed, rendering its reconstitution impossible.

3.4. ACCESS

JHCSC shall ensure that only authorized personnel have access to the personal data of its faculty. Access will be strictly limited to what is necessary for the fulfillment of their respective duties related to the processing of that personal data. Additionally, access to personal data will adhere to the JHCSC Data Classification Policy, ensuring compliance with established guidelines for data protection and privacy.

3.5. DISCLOSURE

JHCSC may send text messages or emails to faculty for purposes related to work, operations, health, emergencies, and community matters. Online meetings may also be utilized to communicate and discuss work-related issues, especially in situations involving work-from-home arrangements.

This arrangement is based on the assumption that staff and personnel have consented to JHCSC gathering their contact information for the purpose of facilitating communication necessary to fulfill work assignments. Compliance with the State College data privacy, security, and confidentiality policies is essential when using text messaging and email platforms.

Only authorized personnel at JHCSC may disclose or transfer personal data, both within the State College and to external entities, provided that such actions remain consistent with the fundamental principles of data privacy.

(4) CONSENT

Generally, a data subject's consent is a prerequisite for the lawful processing of their personal data. However, this requirement is not absolute, and under the following conditions, JHCSC may process a staff member's personal data without obtaining consent:

- (1) The processing of personal information is necessary and related to the fulfillment of a contract with the data subject or to take steps at the request of the data subject prior to entering into a contract.
- (2) The processing is necessary for compliance with a legal obligation to which JHCSC, as the personal information controller, is subject.
- (3) The processing is necessary to protect vitally important interests of the data subject, including life and health.
- (4) The processing is necessary to respond to a national emergency, to comply with public order and safety requirements, or to fulfill functions of public authority that involve processing personal data in order to carry out the State College mandate.
- (5) The processing is necessary for the legitimate interests pursued by JHCSC or by a third party to whom the data is disclosed, except where such

interests are overridden by the fundamental rights and freedoms of the data subject that require protection under Philippine law.

(5) SECURITY MEASURES

5.1. ORGANIZATIONAL SECURITY MEASURES

JHCSC shall continuously develop and apply appropriate organizational security measures to ensure the confidentiality, integrity, and availability of its staff's personal data. These measures include, but are not limited to, the following:

- (1) JHCSC Privacy Manual
- (2) JHCSC Data Classification Policy
- (3) Remote Work Privacy Guidelines
- (4) Data Protection in Work Processes
- (5) JHCSC Message and Communications Policy
- (6) JHCSC Email Policy
- (7) Other pertinent State College issuances

5.2. PHYSICAL SECURITY MEASURES

JHCSC shall ensure that the physical storage of its staff's personal data is always secured. Access to these storage facilities shall be limited only to authorized personnel.

Furthermore, JHCSC shall ensure that in the course of processing staff's personal data, the physical security measures prescribed by the JHCSC Privacy Manual are observed.

5.3. TECHNICAL SECURITY MEASURES

JHCSC shall apply the appropriate technical security measures to ensure that its staff's personal data remain confidential, available, and unaltered at all times. It shall adopt the necessary provisions on the Technical Security Measures in the JHCSC Data Privacy Manual and the National Privacy Commission's Circular on the Security of Personal Data in Government Agencies.

(6) RIGHTS OF DATA SUBJECT

6.1. RIGHT TO BE INFORMED

Every faculty member has the right to be informed about the purpose of collecting, using, disclosing, and processing their personal data. This encompasses how the data will be processed and the offices or units responsible for handling it.

6.2. RIGHT TO ACCESS

Every faculty member has the right, in accordance with relevant laws and JHCSC regulations, to reasonable access to their personal data processed by the College.

6.3. RIGHT TO OBJECT AND RIGHT TO CORRECT OR RECTIFY

Every faculty member has the right to challenge the accuracy of their personal data and to have it rectified or corrected.

6.4. RIGHT TO ERASURE OR BLOCKING

The rights to erasure and blocking do not apply to personal data, documents, records, and accounts that are part of JHCSC's public records as an instrumentality of the government or as a State College. However, these rights may be exercised if there is substantial proof that the processing of personal data is unlawful.

6.5. RIGHT OF DATA PORTABILITY

Every faculty member has the right, subject to relevant laws and JHCSC rules and regulations, to request a copy of their personal data in a commonly used format that allows for further use.

6.6. RIGHT TO FILE A COMPLAINT AND RIGHT TO DAMAGES

Every faculty member has the right to file a complaint if their personal information has been misused, maliciously or improperly disclosed, or if any of the aforementioned rights have been violated. They also have the right to be indemnified for any damages suffered due to such violations.

(7) GROUP CHATS

Group chats among faculty members are commonly used to facilitate communication and collaboration. However, these platforms may also involve the sharing of personal data or sensitive information, requiring adherence to data

privacy principles. JHCSC establishes the following policy for group chats among faculty:

- 7.1. Group chats should be used exclusively for academic, administrative, or professional purposes. Faculty members must avoid sharing personal opinions or unrelated content that could compromise professionalism.
- 7.2. Personal information of students, colleagues, or third parties must not be disclosed in group chats unless it is strictly necessary for legitimate purposes and authorized by the relevant parties.
- 7.3. Sensitive information, such as grades or disciplinary actions, must only be shared through secured and approved channels, not through group chats
- 7.4. Only authorized faculty members may join group chats. Membership lists should be regularly reviewed to ensure only current and relevant participants remain in the group.
- 7.5. Faculty members should use official or institution-approved communication platforms that comply with data privacy standards.
- 7.6. Chats that involve institutional matters or official decisions must be archived or recorded as necessary, following data retention policies. Informal or personal group chats should not contain institutional data.
- 7.7 Any suspected breach of confidentiality or inappropriate use of the group chat must be reported immediately to the designated Data Privacy Officer for investigation.

PRIVACY POLICY FOR ALUMNI AND DONORS

RATIONALE

In recognition of the constitutional and inherent right of individuals to privacy, J.H. Cerilles State College ("JHCSC") affirms its commitment to protect and uphold the privacy of personal information through this JHCSC Privacy Policy for Alumni and Donors.

This Policy is a derivative of and subject to the overarching JHCSC Privacy Policy.

I. COVERED BY THIS POLICY

This Policy governs JHCSC Alumni and Donors, including donees, whose personal information, sensitive personal information, and privileged information ("Personal Data") are processed by JHCSC.

II. REASON OF PERSONAL DATA PROCESSED

2.1. JHCSC processes Personal Data to –

Perform its obligations, exercise its rights, and conduct its associated functions as:

- (1) a government instrumentality; a higher education institution; a juridical entity with its own rights, interests, and internal and external affairs. (2) For each particular unit of JHCSC, conduct all acts reasonably foreseeable from and customarily performed by similar institutions.

III. TYPES OF PERSONAL DATA PROCESSED

3.1. JHCSC processes Personal Data of Alumni and Donors including but not limited to:

- (1) Personal details such as name, date of birth, gender, civil status, and affiliations; Contact information such as address, email, mobile, and telephone numbers; Employment information such as government-issued identification numbers, position, and functions;

3.2. JHCSC processes other Personal Data of Alumni and Donors necessary for the following purposes (the “Purposes”):

3.2.1. Alumni engagement purposes such as:

- (1) Maintenance of alumni database for networking and job placement;
- (2) Tracking career paths and achievements of alumni;

3.2.2. Donation management such as:

- (1) Compliance with legal requirements, including the filing of tax returns and adherence to anti-money laundering laws;
- (2) Recording sources and allocation of donations for transparency in the College’s funds;

3.2.3. Creation, updating, and maintenance of records and accounts;

3.2.4. Security and community affairs management; and

3.2.5. Purposes necessary for JHCSC to fulfill its obligations, exercise its rights, and conduct its functions as a higher education institution, a government instrumentality, and a juridical entity with its own rights, interests, and both internal and external affairs.

IV. PROCESSING AND RETENTION OF PERSONAL DATA AT JHCSC

4.1. JHCSC processes and retains Personal Data as necessary for the Purposes in accordance with:

- (1) The Data Privacy Act of 2012, the National Archives of the Philippines Act of 2007, and their Implementing Rules and Regulations;
- (2) Policies, guidelines, and rules of the JHCSC on data privacy, research, and ethical codes of conduct; and
- (3) Executive and regulatory issuances, including those on Freedom of Information.

V. PERSONAL DATA STORED AND TRANSMISSION

Personal Data are stored in physical and electronic "Data Processing Systems" of JHCSC as defined under National Privacy Commission Circular No. 17-01. Personal Data are transmitted in accordance with Chapter III of the Data Privacy Act of 2012 and Rule V of its Implementing Rules and Regulations.

VI. RIGHTS AND RESPONSIBILITIES OF ALUMNI AND DONOR

The rights and responsibilities of Alumni and Donors are governed by the JHCSC Data Privacy under Subject Rights and Responsibilities.

(5) EFFECTIVITY AND DEFINITION OF TERMS

The effectivity of this policy and the definition of terms used here are those adopted in the JHCSC Privacy Policy.

(6) DATA PROTECTION OFFICER

For data protection concerns or to report privacy incidents, please contact the JHCSC Data Protection Officer.

PRIVACY POLICY FOR APPLICANT

RATIONALE

As the State College of Province of Zamboanga del Sur, J.H. Cerilles State College (JHCSC) conducts admission processes for students and recruitment processes for faculty and staff. In the course of these activities, JHCSC collects, uses, retains, and disposes of personal information from applicants. Therefore, it is the responsibility of the State College to protect the personal information of its applicants.

This Derivative Policy aims to outline and discuss how the State College handles the processing of applicants' personal information in accordance with the Data Privacy Act of 2012.

I. DEFINITION OF TERMS

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

- 1.1. **Applicant** refers to individuals whose applying as Student, Faculty, or Staff of the State College;
- 1.2. **Data Privacy Act (DPA)** refers to Republic Act No. 10173 or the Data Privacy Act of 2012;
- 1.3. **Data Processing System** refers to either computerized system or physical records which stores, processes or transmits personal information or sensitive personal information owned or managed by UP Diliman unit or office;
- 1.4. **Data Subject** refers to an individual whose personal information is processed. For the purposes of this Policy, the term Data Subject shall refer to the applicant Students, Faculty, and Staff;
- 1.5. **IRR** refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
- 1.6. **NPC** refers to the National Privacy Commission of the Philippines as created by the Data Privacy Act of 2012;
- 1.7. **Personal Data** refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012;
- 1.8. **Processing** refers to any operation or any set of operations performed upon personal information, including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data; and

1.9. **Units and Offices** refer to JHCSC academic units and administrative offices.

II. PRINCIPLES OF DATA PRIVACY IN RELATION TO THE PROCESSING OF THE APPLICANT'S PERSONAL DATA

2.1. TRANSPARENCY

The J.H. Cerilles State College shall process the personal information of its applicants only after ensuring that they are informed of the identification of the unit or office collecting their personal data, as well as the nature, purpose, and extent of its processing.

2.2. LEGITIMATE PURPOSE

The State College shall process its data subjects' personal information solely in accordance with its declared and specified purposes. Additionally, this processing must comply with laws, morals, public policy, and relevant issuances of the State College.

2.2.1. The State College processes personal data on the following grounds:

In the performance of its obligations, exercise of its rights, and conduct of its associated functions as a:

- (1) Government instrumentality
- (2) Higher education institution

2.2.2. In pursuit of its purpose and mandate under Act No. 1870 and Republic Act No. 9500

2.2.3. In the conduct of all acts that are reasonably foreseeable and customarily performed by similar entities

2.2.4. For decisions and actions that promote the holistic welfare of its students, their parents and guardians, faculty, staff, researchers, alumni, and the broader community of J.H. Cerilles State College

2.2.5. For the management and administration of its internal and external affairs as an academic and research institution, government instrumentality, and juridical entity with its own rights and interests.

Corollary to this, the State College processes the collected personal data in accordance with the following laws:

- (1) The Data Privacy Act of 2012

- (2) The National Archives of the Philippines Act of 2007, including its Implementing Rules and Regulations and other relevant issuances
- (3) The J.H. Cerilles State College Privacy Manual
- (4) The J.H. Cerilles State College Records Management Policy
- (5) Policies, guidelines, and rules of the J.H. Cerilles State College System
- (6) Executive Order No. 2, series of 2016, concerning the Freedom of Information and related issuances
- (7) Other applicable laws or regulations that pertain to or amend the aforementioned provisions.

2.3. PROPORTIONALITY

The State College shall consistently adhere to the principle of data minimization, ensuring that it only processes personal data that is accurate, relevant, and necessary for the specified purposes.

Moreover, it will refrain from processing personal data if the intended purposes can be reasonably achieved through alternative means.

III. PROCESSING OF PERSONAL DATA

3.1. COLLECTION OF PERSONAL DATA

Collection of Applicant's personal data at J.H. Cerilles State College may be conducted through various data-gathering forms, including but not limited to written records (e.g., Personal Data Sheet) and photographic and video images.

The collected personal data may include any of the following:

- (1) Personal Details: (e.g., name, date of birth, sex, civil status)
- (2) Contact Information: (e.g., mobile number, email address, home address)
- (3) Academic Information: (e.g., educational background, scholastic records)
- (4) Employment Information: (e.g., Tax Identification Number (TIN), Philhealth ID Number, GSIS Membership, employee number)
- (5) Applicant Information: (e.g., former employment history, affiliations)

- (6) Medical Information: (e.g., physical examination, psychiatric evaluation, and drug test results)
- (7) Photographs or Videos: (e.g., for the official documentation of College activities or events)

3.2. USE OF PERSONAL DATA

The use of the Applicant's personal data at JHCSC shall always align with the State College mandate. Specifically, the use of personal data may include the following:

- (1) Academic, research, extra-curricular, student welfare, and disciplinary purposes.
- (2) Administrative disciplinary purposes.
- (3) Supervision of academic and research endeavors.
- (4) Management of human resources and supervision of work conduct.
- (5) Employee application processing and identity verification.
- (6) Documentation and record-keeping.
- (7) Customer, client, patient, or community service initiatives.
- (8) Performance evaluation.
- (9) Documentation of the JHCSC's official activities and events.
- (10) Recognition and awards.
- (11) Identification of the necessity and legality of the purposes prior to or at the time personal information is collected, used, and disclosed.
- (12) Other similar purposes that align with the JHCSC mandate.

3.3. STORAGE, RETENTION, DISPOSAL AND DESTRUCTION OF PERSONAL DATA

JHCSC shall ensure that all personal data it collects and uses are stored in secure facilities to prevent unauthorized access or use. The State will implement necessary physical, organizational, and technical security measures to maintain the confidentiality, availability, and integrity of the stored personal data.

The retention of staff personal data will be limited to the duration necessary to comply with applicable laws, rules, and regulations, including National Archives' Circulars and JHCSC's Records Management Policy.

When the time for retention has expired, personal data will be disposed of and destroyed in a manner that ensures no part of the data is exposed, rendering its reconstitution impossible

3.4. ACCESS

JHCSC shall ensure that only authorized personnel have access to the personal data of its applicant. Access will be strictly limited to what is necessary for the fulfillment of their respective duties related to the processing of that personal data. Additionally, access to personal data will adhere to the JHCSC Data Classification Policy, ensuring compliance with established guidelines for data protection and privacy.

3.5. DISCLOSURE

Only authorized personnel at JHCSC may disclose or transfer personal data, both within the State College and to external entities, provided that such actions remain consistent with the fundamental principles of data privacy.

IV. CONSENT

Generally, a data subject's consent is a prerequisite for the lawful processing of their personal data. However, this requirement is not absolute, and under the following conditions, JHCSC may process an applicant member's personal data without obtaining consent:

- (1) The processing of personal information is necessary and related to the fulfillment of a contract with the data subject or to take steps at the request of the data subject prior to entering into a contract.
- (2) The processing is necessary for compliance with a legal obligation to which JHCSC, as the personal information controller, is subject.
- (3) The processing is necessary to protect vitally important interests of the data subject, including life and health.
- (4) The processing is necessary to respond to a national emergency, to comply with public order and safety requirements, or to fulfill functions of public authority that involve processing personal data in order to carry out the State College mandate.
- (5) The processing is necessary for the legitimate interests pursued by JHCSC or by a third party to whom the data is disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject that require protection under Philippine law.

V. SECURITY MEASURES

5.1. ORGANIZATIONAL SECURITY MEASURES

JHCSC shall continuously develop and apply appropriate organizational security measures to ensure the confidentiality, integrity, and availability of its staff's personal data. These measures include, but are not limited to, the following:

- (1) JHCSC Privacy Manual
- (2) JHCSC Data Classification Policy
- (3) Remote Work Privacy Guidelines
- (4) Data Protection in Work Processes
- (5) JHCSC Message and Communications Policy
- (6) JHCSC Email Policy
- (7) Other pertinent State College issuances

5.2. PHYSICAL SECURITY MEASURES

JHCSC shall ensure that the physical storage of its staff's personal data is always secured. Access to these storage facilities shall be limited only to authorized personnel.

Furthermore, JHCSC shall ensure that in the course of processing staff's personal data, the physical security measures prescribed by the JHCSC Privacy Manual are observed.

5.3. TECHNICAL SECURITY MEASURES

JHCSC shall apply the appropriate technical security measures to ensure that its staff's personal data remain confidential, available, and unaltered at all times. It shall adopt the necessary provisions on the Technical Security Measures in the JHCSC Data Privacy Manual and the National Privacy Commission's Circular on the Security of Personal Data in Government Agencies.

VI. RIGHTS OF DATA SUBJECT

6.1. RIGHT TO BE INFORMED

Every staff member has the right to be informed about the purpose of collecting, using, disclosing, and processing their personal data. This encompasses how the data will be processed and the offices or units responsible for handling it.

6.2. RIGHT TO ACCESS

Every staff member has the right, in accordance with relevant laws and JHCSC regulations, to reasonable access to their personal data processed by the College.

6.3. RIGHT TO OBJECT AND RIGHT TO CORRECT OR RECTIFY

Every staff member has the right to challenge the accuracy of their personal data and to have it rectified or corrected.

6.4. RIGHT TO ERASURE OR BLOCKING

The rights to erasure and blocking do not apply to personal data, documents, records, and accounts that are part of JHCSC's public records as an instrumentality of the government or as a State College. However, these rights may be exercised if there is substantial proof that the processing of personal data is unlawful.

6.5. RIGHT OF DATA PORTABILITY

Every staff member has the right, subject to relevant laws and JHCSC rules and regulations, to request a copy of their personal data in a commonly used format that allows for further use.

6.6. RIGHT TO FILE A COMPLAINT AND RIGHT TO DAMAGES

Every staff member has the right to file a complaint if their personal information has been misused, maliciously or improperly disclosed, or if any of the aforementioned rights have been violated. They also have the right to be indemnified for any damages suffered due to such violations.