Republic of the Philippines
Department of Science and Technology
PHILIPPINE SCIENCE HIGH SCHOOL SYSTEM
(DOST-PSHS SYSTEM)

PSHS System – Data Privacy Manual

In Compliance to R.A. No. 10173, also known as the Data Privacy Act of 2012 (DPA)

October 2020

A. Background

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.

It ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

This document is an internal issuance meant for the use and application of PSHS personnel to guide them on how to deal with and process information and data collected from its clients and stakeholders.

B. Introduction

The PSHS System hereby adopts this Data Privacy Manual in compliance with Republic Act No. 10173 otherwise known as Data Privacy Act of 2012 (DPA), and its Implementing Rules and Regulations and other relevant policies and issuances of the National Privacy Commission, with the end in view of protecting and upholding the fundamental human right of privacy of students, their parents or guardians, employees and other third parties while ensuring free flow of information in accordance with Executive Order No. 02 s. 2016 or the Freedom of Information Act. Towards this end, the PSHS System assures all its stakeholders that all personal information and data collected from them are processed pursuant to the general principles of transparency, legitimate purpose and proportionality as stipulated in the DPA.

This manual aims to inform all PSHS System stakeholders and clients of their privacy rights, and the various privacy measures and data protection protocols adopted by the PSHS System in order for them to exercise those rights, and build their confidence with regard to the security and protection of their personal data under the custody by the PSHS System.

C. Definition of Terms

Terms used in the Manual must be defined for consistency and uniformity in usage. This portion will make sure of that, and allow users of the Manual to understand the words, statements, and concepts used in the document.

1) **"Authorized Personnel"** refers to employee/s or officer/s of the PSHS System authorized to collect, access and/or process Personal Data either by the function of their office, unit, division, or position, or through specific authority given in accordance with the policies of the PSHS System.

2) **"Compliance Officer for Privacy" or "COP"** refers to an individual duly authorized by the PSHS System to perform some of the DPO's functions for a campus, office, unit, division, or any of its subdivision.

3) **"Consent of the Data Subject"** refers to any freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and processing of his/her personal, sensitive personal, or privileged information over a specific purpose. It shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of a Data Subject by a lawful representative or an agent specifically authorized by the Data Subject to do so.

4) **"Data Privacy Response Team"** refers to the group of individuals designated by the PSHS System to respond to inquiries and complaints relating to data privacy, and to assist in ensuring the PSHS System's compliance with the Data Privacy Act, its IRR, and any other government-issued data privacy regulations and issuances, as well as implementing this Manual.

5) **"Data Processing Systems"** refers to the structure and procedure by which Personal Data is collected and further processed by the PSHS System in its Information and Communications System/s and/or relevant Filing System/s, including the purpose and intended output of the Processing.

6) **"Data Protection Officer" or "DPO"** refers to the officer duly designated by the PSHS System to be accountable for the latter's compliance with the Data Privacy Act, its IRR, and any other government issued data privacy regulations and issuances, as well as implementation of the Manual.

7) **"Data Sharing"** refers to the disclosure or transfer to a third party of Personal Data under the control or custody of the PSHS System.

8) **"Data Sharing Agreement"** refers to any written contract or agreement that contains the terms and conditions of a data sharing arrangement entered into by the PSHS System.

9) **"Data Subject"** refers to an individual whose Personal, Sensitive Personal, and/or Privileged Information are processed. It refers to PSHS System's clients, students and their parents or guardians, employees (regardless of their employment status), members of the Board of Trustees and their duly appointed representatives, consultants, suppliers, subcontractors, office visitors, and other persons whose information are collected and processed by the PSHS System as an integral and necessary part of its operations.

10) **"Filing System"** refers to any structured set of personal data that are accessible according to specific criteria whether centralized, decentralized or dispersed on a function or geographical/ campus basis.

11) **"Information and Communications System"** refers to a system for generating, sending, receiving, storing, or otherwise Processing electronic data messages, or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.

12) **"Outsourcing"** refers to the disclosure or transfer of Personal Data by the PSHS System to a Personal Information Processor for the latter's Processing upon the instructions of a duly authorized person.

13) **"Outsourcing Agreement"** refers to any written contract entered into by the PSHS System with a Personal Information Processor, including its service providers.

14) **"Personal Data"** refers to all types of Personal Information collected and processed by the Company. Personal Data may be classified as follows:

    a) **"Confidential Personal Data"** pertain to all other information to which access is restricted, and of which Processing requires the written consent of the Data Subject concerned, such as but not limited to Employee 201 files and information contained therein, device passwords and/or passcode, bank account numbers, ATM card numbers, credit card numbers, and the like. It also includes Personal Information and Sensitive Personal Information; and

    b) **"Public Personal Data"** pertain to Personal Information of a Data Subject which may be disclosed to the public by the PSHS due to, or as required by, its operations, and for government regulatory compliance and company disclosures.

15) **"Personal Data Breach"** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. A Personal Data Breach may be in any of the following nature:

    a) **"Availability Breach,"** which results from the loss of, or accidental or unlawful destruction of Personal Data;

    b) **"Confidentiality Breach,"** which results from the unauthorized disclosure of, or access to Personal Data; and/or

    c) **"Integrity Breach,"** which results from the alteration of Personal Data.

16) **"Personal Information"** refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information, would directly and certainly identify an individual.

17) **"Personal Information Controller" or "PIC"** refers to a natural or juridical person, or any other body, including the PSHS System who/which controls the processing of Personal Data, or instructs another to process Personal Data on its behalf.

18) **"Personal Information Processor or "PIP"** refers to any natural or juridical person, or any other body, to whom a PIC, including the PSHS System, outsources, or gives instructions as regards, the Processing of Personal Data pertaining to a Data Subject.

19) **"Privacy Policy"** refers to the internal statement that governs the PSHS System's practices of handling Personal Data. It instructs the users of Personal Data (i.e., Authorized Personnel) on the processing of Personal Data and informs them of the rights of the Data Subjects.

20) **"Privacy Notice"** refers to the statement addressed to a Data Subject to inform him/her of how PSHS processes his/her Personal Data.

21) **"Privileged Information"** refers to any and all forms of data, which, under the Rules of Court and other pertinent laws, constitute privileged communication.

22) **"Processing"** refers to any operation or any set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction thereof. Processing may be performed through automated means or by manual processing.

23) **"PSHS System"** as defined in R.A. 8496 as amended by R.A. 9036, refers to the Office of the Executive Director and all PSHS Campuses, including all units, offices, and divisions therein.

24) **"PSHS System Quality Management System Manual"** or QMS refers to the operational manual of the PSHS System which consists of Six (6) separate manuals:

    a) Systems Operations Manual (SOM)
    b) Student Services Manual (SSM)
    c) Finance and Administrative Manual (FAM)
    d) Quality Manual (QM)
    e) Student Affairs Manual (SAM)
    f) Curriculum Instruction Manual (CIM)

25) **"School Records"** refer to the records of students of all acts, events, accomplishments, results or research and all documents depicting the various activities of the students. This include but not limited to the following records:

a) Personal and background information
b) Academic records/ reports
c) Financial information and records (e.g. stipend received scholarship categories and supporting documents thereto, etc.)
d) Disciplinary records
e) Medical records including psychological profile
f) Admission records
g) Attendance registers
h) Student achievement and/ or test results

26) **"Security Incident"** is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of Personal Data. It includes incidents that would result to a Personal Data Breach, if not for safeguards that have been put in place.

27) **"Security Measures"** refers to the Physical, Technical, and Organizational measures employed by the Company to protect Personal Data from natural and human dangers.

28) **"Sensitive Personal Information"** refers to Personal Information:

a) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;

b) About an individual's health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

c) Issued by government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension, or revocation, and tax returns; and

d) Specifically established by an executive order or an act of Congress to be kept classified.

D. Scope and Limitations

This manual is an internal issuance meant for the use and application PSHS Personnel on how to deal with and process all information/ data collected from its clients and stakeholders. It covers all campuses, divisions, offices, and units under the PSHS System, and applies to all data that the PSHS System holds relating the identifiable individuals regardless of their status or type of employment, stakeholders and other clients.

E. Data Privacy Principles

The PSHS System abides by the following principles in the processing of all personal data from the time of its collection, to their actual storage or retention, and destruction:

a) **Transparency.** The Data Subject shall be informed of the nature, purpose, and extent of the Processing of his/her Personal Data, including the risks and safeguards involved, the identity of the Company, his/her rights as a Data Subject, and how these may be exercised.

b) **Legitimate Purpose.** The Processing of Personal Data shall only be for the purpose declared and specified to the Data Subject. No further Processing of Personal Data shall be done without the consent of the Data Subject.

c) **Proportionality.** The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data will be processed by the PSHS System only if the purpose of the Processing could not be reasonably fulfilled by other means, and if required by the PSHS System's operations.

F. Processing of Personal Data

In the processing of data, the PSHS System shall observe the following general principles in every stage of the data life cycle -- from the collection of personal data, to their storage, retention, and destruction:

a) **Data Collection : Informed Consent and Notificaton.** All sensitive personal data/ information being requested or collected from data subject(s) must have the explicit consent of the latter. Further, data subject(s) must be informed of the type and purpose of the data being collected from them thru a privacy statement/ notice, and that such data are indicated in the prescribed forms being used to collect the data.

   i. The Data Privacy Officer (DPO) and Personal Information Controller (PIC) shall be responsible for personal information under its control or custody, and shall be accountable for complying with the requirements of the DPA.
   ii. The DPO/ PIC shall determine the type of data to be collected, the mode of collection to employ, the frequency of data collection, and related others; and communicate these things to the PIP who shall be responsible for collecting the data/ information in accordance with approved protocols.
   iii. Data collected may be in a form of hard copy or e-copy which shall be consolidated by the PIP/PIC.
   iv. If the data subject noted an erroneous data collected; he/ she has the right to file for correction/ erasure using the prescribed form.

b) **Use of data.** Only authorized PSHS System personnel are allowed to access, use and process data/ information collected from data subject for legitimate primary or secondary purposes of the school for which they were collected or intended for use as stated in the forms or documents signed by the students, third parties or employees as the case may be.

   i. **Primary Purpose.** To provide scholars with the best teaching and learning experience possible, the PSHS System through its teachers, guidance counselors, registrar, regularly collects student data as an integral part of its function. Such information are used to monitor students' progress, improve instruction, provide basis for feedback, measure student performance and overall satisfaction, enhance the quality of school services, monitor mental health and behavioral changes, enhance the overall teaching and learning environment, and others.

      Collection, use, retention, storage and disposition of student records shall be conducted in accordance with existing and applicable policy manuals using the prescribed forms as per PSHSS-QMS Manual.

   ii. **Secondary Purpose.** Data/ information from stakeholders are also collected and used for: compliance to government and regulatory reportorial requirements such as to the Department of Science and Technology (DOST), Commission on Audit (COA), Civil Service Commission (CSC), Department of Education (DepEd), facilitation of administrative processes (clearance, stipend, allowance), evaluation of individual and organizational performance, assessment of suppliers' and contractor's performance, research purposes (numbers and statistics), provision of employee benefits including but not limited to magna carta benefits for Science and technology personnel, and other similar purposes not directly related to teaching and learning.

      Employee's personal data are collected in compliance with reportorial and administrative requirements of the Civil Service Commission, Labor Law, and related issuances, with reference to FAM 4.14 to 4.16.

c) Storage, Retention, Destruction and Disposition. Responsible persons shall ensure that personal data under their custody are protected against any accidental or unlawful destruction, altercation and disclosure against any unlawful processing. The PSHS System shall implement appropriate security measures including but not limited to electronic back-up systems in storing and retrieving information as well as passwords at different levels of authorized access.

The period of retention of data and the destruction/ disposition thereof shall be conducted in accordance with the PSHS System's Record Disposition Schedule (RDS), and applicable provisions and rules under the National Archives of the Philippines, and related government issuances.

G. Authorized Access

Only authorized PSHS personnel can access, pull-out, duplicate copies, share, disclose and distribute personal and sensitive data/ information, for a lawful purpose.

Annex C of the PSHS System Freedom of Information *Manual* provides a list of highly sensitive data/ information deemed confidential by the PSHS System and is outside the purview of the FOI Act. Access to these data without proper authorization is strictly prohibited, as such the contents of those documents may not be disclosed or shared to any person, except when there is an order from a competent court, or when public safety requires otherwise.

All PSHS personnel shall maintain the confidentiality and secrecy of all personal data that come their knowledge and possession even after resignation, termination of contract, or other contractual relations. Personal data under the custody of the company shall be disclosed only pursuant to a lawful purpose, such as complying with court orders, subpoenas, and/or other legal obligations.

H. Security Measures

The PSHS System thru its duly designated PICs/ PIPs is committed to implementing reasonable and appropriate physical, technical and organizational measures for the protection of personal data, including but not limited to security measures aimed at maintaining the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

A. Organization Security Measures

i. **Designation of Data Protection Officers/ Compliance Officer for Privacy** who shall be accountable for the organization's compliance with the DPA, its IRR and any other government issued data privacy regulations and issuances, as well as the implementation of this manual.

ii. **Designation of PICs** who shall be responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

iii. **Conduct of trainings or seminars** for DPOs/ CPOs, PICs and PIPs to keep them updated on developments in data privacy and security

iv. **Conduct of Privacy Impact Assessment (PIA).** The PSHS shall periodically conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data.

v. **Institutionalization of Recording and Documentation of Activities.** The protocols for recording, filing and documentation of records, including all forms used by the PSHS System in collecting data from data subjects are outlined in the PSHS-QMS Manual. The general policy guidelines which stipulates the use of: Forms (Masterlist of Forms), Filing Charts, Document Logs/ Legers and others, are outlined in QM 13.1.

vi. **Duty of Confidentiality.** All employees with access to personal sensitive information shall be asked to sign an Non-Disclosure Agreement, prohibiting them from disclosing any such data/ information to the public without proper approval.

vii. **Review of Privacy Manual.** This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

The PSHS System is committed to adopting physical measures intended to monitor and limit access to the facility containing the personal data, including the activities therein. Further, in order to ensure that mechanical destruction, tampering and alteration of personal data under the custody of the organization are protected from man-made disasters, power disturbances, external access, and other similar threats, the PSHS System has instituted Disaster Risk Management procedures (FAM 7.1), Incidence Command System (FAM 15.0), Public Service Continuity Plan (FAM 16.0), Information Technology Processes and Back-up Systems (FAM 12.1) among others.

i. **Format of data to be collected.** All forms used in the collection of student, employees, and third parties is strictly controlled and updated in accordance with QM 13.1 (Control of Documented Information), and listed in the PSHS Masterlist of Forms with their corresponding code or control number.

ii. **Filing of Records.** Personal data in the custody of records officers and process owners are coded and filed in accordance with the PSHS System's Quality Manual – Filing Charts, which are kep in digital/electronic format and paper-based/physical format.

iii. **Provision of Storage Facilities, Type and Location.** Records Officers and Process Owners of the PSHS System has been provided with filing cabinets (with locks), electronic storage system, personal data room/separate room, and similar other storage facilities where they can store and secure all records in their custody. Highly confidential documents are stored in a *"Strong Room".*

iv. **Access procedure of agency personnel.** Only authorized personnel are allowed inside the data room. Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

v. **Design of office space/work station.** The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

vi. **Retention and disposal procedure.** Retention and disposal of records are done in accordance with the PSHS System Records Disposition Schedule, and existing guidelines from the National Archives of the Philippines.

C. Technical Security Measures

The PSHS System is committed to implementing best practices in data security, and set up appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access.

i. **Modes of transfer of personal data within the organization, or to third parties.** Electronic mails sent thru the PSHS mail server contains a privacy and confidentiality statement, and are transferred using a secured connection (SSL/ TSL) email facility with encryption of the data, including any or all attachments. Another way to which data will be shared is upon request of the data subject or through her/his authorized agent or guardian and this is done through an authorization. Examples of this would be requests for copy of Transcript of Records, Diploma, clearance, certificate of employment, and other related documents which may be needed in order for the student or PSHS personnel to be accepted in other schools or offices.

ii. **Monitoring for security breaches.** The PSHS System thru the iGovPhil Program - Security Operations Center which hosts the PSHS website uses an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system. The iGovPhil Program-SOO also conducts periodic vulnerability management, log analysis/ monitoring, network security monitoring, fine tuning, incident handling, security incident escalation, penetration testing, among others on government websites hosted in their servers.

iii. **Assessment and review of software application.** To ensure the compatibility and security of applications installed in work units, only responsible personnel (i.e. designated ISAs/ MIS) are allowed to install applications in computers pursuant to FAM 12.1 (Information Technology Management).

iv. **Encryption, authentication process.** Computer units in the PSHS System are password protected to control and limit access to personal data.

v. **Data recovery and Back-up Systems.** Data recovery of digital files, and Data Back-up are conducted periodically in accordance with FAM 12.3 (Back-up and Recovery of Digital Files).

I. Inquiries and Complaints

As a matter of policy, the PSHS System acknowledges the following rights of data subject in accordance with law:

a) Right to reasonable access to his or her personal data being processed by the personal information controller or personal information processor.

b) Right to dispute the inaccuracy or error in the personal data;

c) Right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and

d) Right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data.

Feedback, Inquiries, Comments and Complaints may be sent via email to the office of the Executive Director at oed@pshs.edu.ph or via telephone: (02)8939-7747, or via correspondence: Office of the Executive Director, Agham Road, Diliman, Quezon City, or thru concerned PSHS Campus Directors whose contact details may be found in their respective websites.

Complaints shall be filed in three (3) printed copies, and sent to the concerned PSHS campus, office, department or unit who shall confirm with the complainant its receipt of the complaint, and process it in accordance with DOST Administrative Order No. 005 series of 2008 otherwise known as *"Rules of Procedures for Disciplinary Cases in the DOST System",* supplemented by the CSC Omnibus Rules on Appointments and Other Human Resources Actions, and related issuances.

OFFICE DIRECTORY

Office of the Executive Director (OED)
Contact No. (02) 8939 7747 / 939 7726 / 939 7749 / 939 0022
Mobile No. 0920 960 7215

MAIN CAMPUS
Agham Road, Diliman, Quezon City
Tel. Nos.: (02) 8929 1606
Website: http://mc.pshs.edu.ph
E-mail address: ocd.mc@pshs.edu.ph

REGIONAL CAMPUS

ILOCOS REGION CAMPUS
San Ildefonso, Ilocos Sur
Tel. Nos.: (077) 674 1454 / 674 1446 / 726 4190 loc. 102
Website: http://irc.pshs.edu.ph
E-mail Address: admin@irc.pshs.edu.ph

CAGAYAN VALLEY CAMPUS
Bayombong, Nueva Vizcaya
Mobile Nos.: 0975 957 0090 / 0920 243 5155
Website: http://cvc.pshs.edu.ph
E-mail Address: pshscvcampus@gmail.com

CORDILLERA ADMINISTRATIVE REGION CAMPUS
Purok 12, Lime Kiln, Irisan, Baguio City
Mobile Nos.: 0949 880 4115 / 0961 361 6125
Website: http://carc.pshs.edu.ph
E-mail Address: ocd.pshscarc@gmail.com

CENTRAL LUZON CAMPUS
Lily Hill St., Clark Freeport Zone, Angeles City
Tel. Nos.: (045) 499 0136 / 499 5597
Mobile Nos.: 0942 266 0139 / 0955 551 7783
Website: http://clc.pshs.edu.ph
E-mail Address: taodiaz@pshs.edu.ph

CALABARZON REGION CAMPUS
Barangay Sampaga, Batangas City
Tel. No.: (043) 724 6199
Mobile No.: 0917 654 8089
Website: http://cbzrc.pshs.edu.ph
E-mail Address: pshscbz@gmail.com

MIMAROPA REGION CAMPUS
Romblon Convention Center, Barangay Rizal, Odiongan, Romblon
Mobile Nos.: 0927 886 6315 / 0939 817 2212 / 0986 149 3980 / 0949 700 1379
Website: http://mrc.pshs.edu.ph
E-mail Address: pshs@mrc.pshs.edu.ph

BICOL REGION CAMPUS
Tagongtong, Goa, Camarines Sur
Tel. No.: (054) 453 2048
Mobile No.: 0929 152 5657
Website: http://brc.pshs.edu.ph
E-mail Address: ocd@brc.pshs.edu.ph

WESTERN VISAYAS CAMPUS
Jaro District, Iloilo City
Tel. Nos.: (033) 329 5644 / 329 2011
Website: http://wvc.pshs.edu.ph
E-mail Address: iloilo@wvc.pshs.edu.ph

CENTRAL VISAYAS CAMPUS
Talaytay, Argao, Cebu
Tel. No.: (032) 485 1000
Mobile No.: 0917 819 1755
Website: http://cvisc.pshs.edu.ph
E-mail Address: ocd@cvisc.pshs.edu.ph

EASTERN VISAYAS CAMPUS
Palo, Leyte
Tel. Nos.: (053) 888 0366 / 888 0359 / 888 0074
Mobile No.: 0939 901 8009
Website: http://evc.pshs.edu.ph
E-mail Address: ocd.evc@pshs.edu.ph

CENTRAL MINDANAO CAMPUS
Nangka, Balo-i, Lanao del Norte
Tel. Nos.: (063) 836 0097 to 98
Mobile No.: 0998 571 6805
Website: http://cmc.pshs.edu.ph
E-mail Address: pshs.cmc.7198@gmail.com

SOUTHERN MINDANAO CAMPUS
Tugbok District, Davao City
Tel. Nos.: (082) 293 0002 / 293 0004
Mobile No.: 0999 718 5180
Website: http://smc.pshs.edu.ph
E-mail Address: info@sms.pshs.edu.ph

SOCCSKSARGEN REGION CAMPUS
Paraiso, Koronadal City, South Cotabato
Mobile Nos.: 0917 319 2797 / 0917 711 0279
Website: http://src.pshs.edu.ph
E-mail Address: ocd@src.pshs.edu.ph

CARAGA REGION CAMPUS
Barangay Tiniwisan - Ampayon, Butuan City
Tel. No.: (085) 817 0987
Website: http://crc.pshs.edu.ph
E-mail Address: official_email@crc.pshs.edu.ph

ZAMBOANGA PENINSULA REGION CAMPUS
Dipolog Sports Complex, Barangay Olingan, Dipolog City
Tel. No.: (065) 212 1616
Mobile No.: 0908 892 9858
Website: http://zrc.pshs.edu.ph
E-mail Address: pshszrcdipolog@gmail.com