


**REVISION HISTORY**

	<b>LA SALLE GREEN HILLS</b>			
	<b>DOCUMENT TITLE:</b> Data Privacy Policy		<b>DOCUMENT NO:</b>	<b>CLASS:</b>
	<b>FILES SOURCE:</b>	<b>EFFECTIVE DATE:</b> 2022 June 18	<b>APPROVAL DATE:</b> 2020 June 18	<b>NO. OF PAGES:</b> 28

**APPROVAL HISTORY**

Date (YYYY-MM-DD)	Prepared by:	Authorized by:	Approved by: (Secondary)	Approved by:
2022 June 18	Atty. Armee M. Javellana <b>RMCO Head Administrator</b>			<i>Br. Edmundo L. Fernandez FSC</i> <b>Br. Edmundo L. Fernandez FSC LSGH President</b>

Revision Date (YYYY-MM-DD)	Author	Reason for Changes
2022 June 15	Atty. Maria Armee M. Javellana Mr. Niccolo Paolo M. Agcaoili Mrs. Esther D. Dollete	In pursuant to the National Privacy Commission directive dated 08 June 2022 to revise the LSGH Data Privacy Policy.

**RELATED INFORMATION**

Document Control No.	Document Title	File Source

**TABLE OF CONTENTS**

Section Title	Page Number
Introduction	2
Objectives	2
Definition of Terms	2
Scope and Coverage	4

Guideline Statements	7
Sanction	24
Annexes	24
References	28

**1. Introduction**

La Salle Green Hills (LSGH) collects, uses, stores and processes personal information relating to potential, current and former employees/personnel and students, parents/guardians, alumni, website users and other relevant third parties, referred to in this policy as data subjects. As Data Privacy has become a relevant and important issue in the education sector and with the implementation of the Data Privacy Act of 2012 (DPA), it is incumbent upon LSGH to adopt reasonable measures to safeguard the personal information it processes. LSGH respects and values data privacy rights and is committed to protect the confidentiality of personal information it collects. This policy sets out how LSGH manages those responsibilities and which trustees, administrators, officers, employees, students and other third party contractors/processors processing personal information should follow to ensure compliance with the DPA and other related legislations and regulations.

**2. Purpose**

This Policy describes a baseline set of common principles governing the handling of Students', Parents', Guardians', Alumni's/Alumnae's, Human Resources' and other third parties' personal information within the institution. These guidelines assure not only the institution's compliance to the Data Privacy Act of 2021, its implementing rules and regulation and other related laws, but will be communicated to its Personnel to ensure their compliance as well.

LSGH values its Students, Parents/Guardians, Alumni/Alumnae, Employee/Personnel and treats their personal information as confidential. In this policy we outline the institution's standards for data subject's personal information privacy practices. LSGH requires, as part of their job responsibility, all its trustees, administrators, offices, personnel and staff entrusted with personal information of data subjects, to treat such (information) as confidential and thus, be in conformity with this policy. LSGH likewise, requires the same responsibility and confidentiality to any third -party service providers that administer and process its personal information.

**3. Objectives**

- 3.1. To ensure clarity and consistency about how personal data must be processed and the expectations of LSGH from all those who process personal data on its behalf.
- 3.2. To ensure compliance with the Data Privacy Act and other relevant legislations and regulations.
- 3.3. To protect LSGH's reputation by ensuring the personal data entrusted to it is processed in accordance with data subject rights.
- 3.4. To protect LSGH from risks of personal data incidents or breaches and other breaches of data protection law.
- 3.5. To embed a culture of privacy that enables compliance.
- 3.6. To promote a culture of trust and respect that enables community building.
- 3.7. To establish effective privacy practices, procedures and systems.
- 3.8. To evaluate LSGH's privacy practices, procedures and systems to ensure continued effectiveness.
- 3.9. To enhance response to privacy issues.
- 3.10. To ensure that information assets receive an appropriate level of protection and clear identification of assets.
- 3.11. To ensure that all employees, permanent or temporary, understand their information security roles and responsibility.
- 3.12. To act as a deterrent to prevent violations, as well as information dissemination to encourage voluntary compliance to organizational Data Privacy and information security policies and procedures.
- 3.13. To reduce the risks of human error, theft, fraud or misuse of school equipment and facilities.

- 3.14. To protect LSGH information and organizational assets from security incidents. and minimize possible Data Privacy Security risks.
- 3.15. To ensure correct and fair treatment of employees/personnel who are suspected of committing Data Privacy or information security breach
- 3.16. To manifest that LSGH is serious in enforcing its Data Privacy or information security policies.

#### 4. **Definition of Terms**

- 4.1. Data Subject -refers to an individual whose personal data is processed by LSGH;
- 4.2. Student – an individual officially enrolled in LSGH;
- 4.3. Former Student – an individual who enrolled but is no longer enrolled in LSGH;
- 4.4. Employees – all employees of LSGH (regardless of type of employment), includes Administrators, Full Time Faculty, Part Time Faculty, Academic Non-Teaching Personnel, Support Staff, Contract based employees, Contractual, Agency Hired and Consultants;
- 4.5. Former employees – employees who are retired, resigned, terminated or contract has ended;
- 4.6. Alumni/Alumnae – an individual who studied in LSGH for at least two (2) years;
- 4.7. Processing – refers to any operation or any set of operations performed upon personal data including, but not limited to, collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;
- 4.8. Processor – individual/department/unit which processes personal data in behalf of LSGH;
- 4.9. Personal Information Controller (PIC) – refers to LSGH, who controls the collection, holding, processing or use of personal data, including a person or organization who instructs another person or organization to collect, hold process, transfer or disclose personal information on his or her behalf;
- 4.10. Personal Information Processor (PIP) – refers to any natural or juridical person qualified to whom a personal information controller may outsource the processing of personal data pertaining to a data subject;
- 4.11. Personal Data – used when personal information, sensitive personal information and privileged information are referred to collectively;
- 4.12. 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;
- 4.13. Sensitive Personal Information – refers to personal information:
  - 4.13.1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
  - 4.13.2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for an offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
  - 4.13.3. Issued by the government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;
  - 4.13.4. Specifically established by an executive order or an act of Congress to be kept classified.
- 4.14. Privileged Information – refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute as privileged communication or includes but not limited to information given by a client to a lawyer, by a patient to a doctor or by a counselee to a counselor;
- 4.15. Consent – refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given in behalf of the data subject by an agent specifically authorized by the data subject to do so;
- 4.16. Privacy as a default setting – systems, processes or practices in LSGH is designed to protect personal data automatically;
- 4.17. Privacy by Design – framework that dictates that privacy and data protection are embedded throughout the entire life cycle of processes, projects, systems and technologies in LSGH, from the early design stage through deployment, use and ultimate disposal or disposition;
- 4.18. Privacy Management Plan – document that identifies specific, measurable goals and targets that identify how LSGH will implement data privacy management for a period of time;

- 4.19. Data Protection Officer (DPO) – refers to the officer designated by LSGH to monitor and ensure LSGH's compliance to the Data Privacy Act and other related laws and regulations and data privacy policies of LSGH. The DPO is also the head of the Data Breach Response Team;
- 4.20. Data Breach Response Team - refers to a group of persons designated by LSGH who are responsible for the following: evaluation of the security incident and deciding on action to be taken including but not limited to restoration of integrity of the information and communication system, mitigation and remediation of any result damage, and compliance with the reporting requirements; coordination with the different departments/units of LSGH for the development of the overall incident response; implementation of the Data Privacy Security Incident Management Policy; reporting actions taken on instances of personal data breaches to the Executive Council;
- 4.21. Personal Data Breach – refers to a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- 4.22. Security Incident – refers to 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 the safeguard that have been put in place;
- 4.23. Privacy Notice – is a notification in a format specified in the appendix of this policy, provided to individuals informing them of the use and purpose for collecting or processing the personal data, and/or allows such individual to consent to such processing of data;
- 4.24. Direct Marketing – refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals. This does not mean it is addressed to a particular person by and but by using other types of personal data (e.g. email address, home address, mobile phone number, etc.)
- 4.25. Third Party Contractors - Any person or entity that receives personal data from LSGH pursuant to contract and other written agreement for purposes of providing services including but limited to data management or storage services.

## 5. **Scope and Coverage**

- 5.1. This policy applies to all departments and units of LSGH, employees/personnel (regardless of classification), students and third party contractors/processors who process personal information collected by LSGH or on behalf of LSGH. The personal data referred to in this policy is limited to those collected and processed by LSGH. This policy applies to all personal data that LSGH processes regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject.
- 5.2. This Policy applies to all personal information of Students, Parents, Guardians, Alumni/Alumnae and Personnel that is collected, maintained or used by trustees, administrators, officers, personnel, staff and third parties and contractors of LSGH.
- 5.3. Personal information that are collected and processed from **students** and **applicants** for admission include but are not limited to the following:
  - 5.3.1. Name
  - 5.3.2. Date and place of birth
  - 5.3.3. Name of parents/guardian
  - 5.3.4. Address
  - 5.3.5. Email address
  - 5.3.6. Telephone/mobile number
  - 5.3.7. Dates of attendance
  - 5.3.8. Grade level
  - 5.3.9. Previous educational institution attended
  - 5.3.10. Date of Graduation
  - 5.3.11. Degrees/Awards/Honors/Scholarships/Grants received
  - 5.3.12. Height and weight information of athletes
  - 5.3.13. Performance records and participation in competitive events and officially recognized activities, sports, and organizations
  - 5.3.14. Photographs/Videos/Images of individual or in groups
  - 5.3.15. Recordings from closed-circuit television
- 5.4. Sensitive Personal Information that is collected from **students** and **applicants** include the following:
  - 5.4.1. Gender
  - 5.4.2. Ethnicity
  - 5.4.3. Religion
  - 5.4.4. Disability/Special Education Needs Conditions

- 5.4.5. Grades
- 5.4.6. Disciplinary records
- 5.4.7. Guidance records
- 5.4.8. Health records
- 5.4.9. Financial records
- 5.4.10. Alien Certificate/Visa/ Passport information of foreign students

\*Students who are 18 years old and above may give his/her parent or guardian consent by signing a Consent to Release Personal Information. In the case that sensitive personal information is collected, expressed written consent is required from the student (if the student is 18 years old and above).

5.5. Student personal information will be used for the following purposes:

- 5.5.1. Processing of student application and enrolment
- 5.5.2. Maintaining student records
- 5.5.3. Managing and evaluating student's academic, deportment and behavioural progress
- 5.5.4. Providing personal advice and support
- 5.5.5. Managing accommodation services such as but not limited to participating in Physical Education classes and Student Intervention Programs
- 5.5.6. Maintaining safety and security
- 5.5.7. Issuance of School identification cards, certifications, transcript of records and the like
- 5.5.8. Providing access to the campus, library and other facilities/services including online access to the school's Learning Management System
- 5.5.9. Providing ancillary services such as uniform, Identification Cards, Learning Management System access and account management, Video conferencing platforms, etc.
- 5.5.10. Providing medical/health services
- 5.5.11. Marketing and publicity of the school
- 5.5.12. Communicating official school announcements
- 5.5.13. Posting and/or publishing of academic, co-curricular and extra-curricular achievements in the school's announcement boards, website, social media sites and publications
- 5.5.14. Providing venues in harnessing and featuring student talents and skills
- 5.5.15. Conducting research for the improvement of programs, services and facilities
- 5.5.16. Analyzing historical and statistical data
- 5.5.17. Maintaining directories and alumni/alumnae records
- 5.5.18. Application/Renewal of Scholarships/ Grants
- 5.5.19. Graduation/Commencement Exercises
- 5.5.20. Joining of school recognized competitions and athletic leagues
- 5.5.21. Processing of student application/ travel requirements for local and international outbound student programs and activities
- 5.5.22. Providing placement services for required on the job training/internship for students
- 5.5.23. Responding to verifications whether an individual is a bona fide student or a graduate of the School and background checks
- 5.5.24. Complying with mandatory reportorial and other lawful requirements of government agencies (Department of Education, Bureau of Immigration, Department of Social Welfare Development, National Youth Commission, National Assessments such as NAT, NCAE, and accrediting associations
- 5.5.25. For membership and accreditation to associations and groups such as but not limited to Philippine Accrediting Association of Schools, Colleges, and Universities (PAASCU), Private Education Assistance Committee (PEAC) and Catholic Educational Association of the Philippines (CEAP).
- 5.5.26. Processing of student applications for colleges and universities

5.6. The School collects personal information from **parents, guardians and/or alumni/alumnae** by filling out LSGH forms.

- 5.6.1. Personal information that are collected and processed from parents or guardians include, but are not limited to, the following:
  - 5.6.1.1. Name
  - 5.6.1.2. Civil Status
  - 5.6.1.3. Addresses
  - 5.6.1.4. Email address
  - 5.6.1.5. Telephone/mobile number
  - 5.6.1.6. Financial information (student accounts status, for scholarship grants application, etc)

- 5.6.2. Personal information collected from **parents, guardians and alumni/alumnae** are for the following purposes:
  - 5.6.2.1. Processing of student school/scholarship application
  - 5.6.2.2. Communicating official school announcements/activities
  - 5.6.2.3. Monitoring student accounts
  - 5.6.2.4. Processing parental consent forms for official student school activities (local and international)
  - 5.6.2.5. Reporting of student's educational progress (if student is below 18 years old or if student is above 18 but has been given consent to parent)
  - 5.6.2.6. Processing of Alumni/Alumnae Records
  - 5.6.2.7. Inviting alumni to participate in student formation activities and development programs
  
- 5.7. Personal information that are collected and processed from **employees/personnel and applicants for employment** which includes, but are not limited to, the following:
  - 5.7.1. Name
  - 5.7.2. Date and place of birth
  - 5.7.3. Addresses
  - 5.7.4. Email address
  - 5.7.5. Telephone/mobile number
  - 5.7.6. Degrees/School/Course/Dates of attendance
  - 5.7.7. Awards/Honors/Scholarships/Grants received
  - 5.7.8. Previous School/Position/Dates of employment
  - 5.7.9. License type/Date passed/License number/current status of license
  - 5.7.10. Professional membership organization/Date of membership
  - 5.7.11. Seminars attended/Inclusive dates
  - 5.7.12. Published works
  - 5.7.13. Dependents' name/date of birth
  - 5.7.14. Photographs/Videos/Images of individual or in groups
  - 5.7.15. Recordings from closed-circuit television
  
- 5.8. Sensitive Personal Information that is collected from **employees/personnel and applicants** include the following:
  - 5.8.1. Gender
  - 5.8.2. Ethnicity
  - 5.8.3. Religion
  - 5.8.4. Marital Status
  - 5.8.5. Disability/Special Needs Conditions
  - 5.8.6. Disciplinary records
  - 5.8.7. Evaluation records
  - 5.8.8. Health records
  - 5.8.9. Financial records
  - 5.8.10. Alien Certificate/Visa/ Passport information of foreign personnel

In case sensitive personal information is collected, expressed written consent is required from the personnel.
  
- 5.9. Personal information collected from **employees/personnel and applicants** is for the following purposes:
  - 5.9.1. Processing of employment application
  - 5.9.2. Job matching
  - 5.9.3. Maintaining personnel records
  - 5.9.4. Compliance with statutory requirements
  - 5.9.5. Providing assistance to foreign workers
  - 5.9.6. Providing access to campus and other facilities
  - 5.9.7. Providing access to online and SMS services
  - 5.9.8. Monitoring of personnel movements
  - 5.9.9. Processing job ranking and promotion
  - 5.9.10. Providing personal growth and development opportunities
  - 5.9.11. Payroll management
  - 5.9.12. Benefits management
  - 5.9.13. Grants management
  - 5.9.14. HMO management
  - 5.9.15. Issuance of School Identification Cards and Certificate of Employment and the like
  - 5.9.16. Ranking/Levelling
  - 5.9.17. Performance evaluation
  - 5.9.18. Awards and Recognition

- 5.9.19. Maintaining safety and security
- 5.9.20. Communicating official school announcements
- 5.9.21. Marketing and publicity of the School
- 5.9.22. Data analytics for strategic planning
- 5.9.23. Compliance to authorizing and accrediting bodies
- 5.9.24. Research for improvement of programs, services and facilities
- 5.9.25. Joining of School activities
- 5.9.26. Posting and/or publishing of personal achievements and/or involvement in School achievements in School's announcement boards, website, social media sites and publications
- 5.9.27. Providing personal advice and support
- 5.9.28. Maintaining directories of employee records
- 5.9.29. Responding to employment verifications
- 5.9.30. Mandatory or voluntary retirement
- 5.10. Personnel personal information is shared internally within the School when appropriate to meet legitimate purposes. Data will only be shared between employees who have the official need to have access to it. All Employees/Personnel of the School shall maintain confidentiality of all personal data that come to their knowledge and possession, even after resignation/retirement, termination of contract, or other contractual relations. Personal data under the custody of the School shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.
- 5.11. Personnel personal information is also shared externally on a need to know basis with the following:
  - 5.11.1. Government agencies (Department of Education (DepEd), DOLE, BIR, SSS, PhilHealth, Pag-Ibig, NPC, DSWD etc.) for purposes of regulation and compliance to the law.
  - 5.11.2. Accrediting agencies such as Philippine Accrediting Association of Schools, Colleges and Universities (PAASCU) for purposes of accreditation
  - 5.11.3. Catholic Educational Association of the Philippines (CEAP) for purpose of retirement contributions
  - 5.11.4. Health Maintenance Organization (HMO) for health/medical insurance

## 6. Guideline Statements

- 6.1. **Data Privacy Security Roles and Responsibilities of Students, Parents, Guardians and Alumni/Alumnae**
  - 6.1.1. All Students, Parents, Guardians and Alumni/Alumnae shall implement and act in accordance with the LSGH Data Privacy and Information Security policies.
  - 6.1.2. All Students, Parents, Guardians and Alumni/Alumnae shall protect information security assets from unauthorized access, disclosure, modification, destruction or interference.
- 6.2. **Guidelines for Students, Parents, Guardians and Alumni/Alumnae**
  - 6.3. **Admissions Process**
    - 6.3.1. The applicant will access the Online Application Form through a link provided in the school's website or the school's official social media accounts.
    - 6.3.2. Digital copies of the admission requirements should be uploaded in the Online Application Form.
    - 6.3.3. Once the required documents have been completed, evaluated and approved, an online interview will be scheduled.
    - 6.3.4. The Admissions result will be emailed after three (3) working days from the interview.
    - 6.3.5. Upon receipt of the acceptance letter, access details will be provided to successful applicants to access the school's Learning Management System for enrollment purposes. Additional details will be sent to parents/guardians regarding enrollment to complete the Admission process.
    - 6.3.6. Data collected from unsuccessful applicants and unenrolled successful applicants will be kept for one school year and after which it will be securely disposed of.
  - 6.4. **Academic Records**  
Data collected from enrolled applicants will be shared with the Registrar's Office and Principal's Office to maintain the applicant's academic records.
  - 6.5. **Medical Clearance**

- 6.5.1. All enrolled students are required to undergo a Medical Examination and Annual Physical Exam.
  - 6.5.2. Medical Certificate and Results will be submitted to the School Clinic.
- 6.6. **Local and International School Sanctioned Travel**  
Students may be asked to provide personal documents such as passport, visa, medical clearance and the like when they join a school activity or get endorsement from the School to participate in an activity that involves travelling.
- 6.7. **School Services and Activities**
- 6.7.1. Students, Parents, Guardian and Alumni/Alumnae may be asked for some of their personal information for them to access services in the School (for example: Learning Resource Center, Finance Resource Department, Health Service Unit, laboratories, etc.)
  - 6.7.2. Students, Parents, Guardian and Alumni/Alumnae may also be asked for other personal information needed for them to be involved in certain activities of the School (for example: retreats, seminars, workshops, social action, formation sessions, etc.)
- 6.8. **Data Privacy Security Roles and Responsibilities of Employees/Personnel**
- 6.8.1. All past, present and prospective employees/personnel, probationary and regular/permanent employees/personnel, contractors, consultants and trainees shall implement their duties and act in accordance with the LSGH Data Privacy and Information Security policies.
  - 6.8.2. All shall protect information security assets from unauthorized access, disclosure, modification, loss, destruction or interference.
- 6.9. **Guidelines for Employees/Personnel**
- 6.9.1. **Pre-Employment Screening**
- 6.9.1.1. The School collects necessary personal information from applicants for employment by filling out application forms with photographs and submitting them together with other documents (resume or curriculum vitae) to the Human Resource Development Office (HRDO).
  - 6.9.1.2. Background verification checks on permanent and temporary employee/personnel and contractors must be carried at the time of processing job applications, especially if a role involves handling information or is in a position of considerable authority. If necessary HRDO shall acquire a consent from the applicant to do background verification.
  - 6.9.1.3. Background verification checks shall be in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, and the perceived risks.
  - 6.9.1.4. All final candidates for employment shall be required to undergo and successfully complete pre-employment screening prior to being employed.
  - 6.9.1.5. Prior to onboarding, additional documents containing personal information (original PSA birth certificate, original PSA marriage certificate, original or certified true copy of transcript of records, certified true copy of diploma, original NBI Clearance, original barangay clearance, photocopy of SSS, Philhealth, Pag-ibig IDs, BIR form 2316, medical exam results, photocopy of PRC license, certificate of employment from previous employer), is collected by the HRDO.
- 6.9.2. **Terms and Conditions of Employment Contract**
- 6.9.2.1. Successful applicants will be asked to sign a contract as well as the Confidentiality and Non-Disclosure Agreement and the HRDO Data Privacy Policy Consent Form. Once hired, HRDO encodes the personal information into their database which may be shared with authorized offices on a need to know basis.
  - 6.9.2.2. All Employees/Personnel and third party contractors are required to sign Confidentiality and Non-Disclosure Agreement of work undertaken during their terms of employment/contract respectively.
  - 6.9.2.3. Employees/Personnel are responsible for notifying the HRDO for any change in their personal information like change of status and contact information on a timely basis. HRDO may require additional



documents to support the updates such as marriage certificate for those newly married, birth certificate for new dependents, certified true copy of diploma for the new graduates, or copy of PRC license for those newly licensed, etc.

6.9.2.4. Faculty shall submit additional documents for ranking, awards and promotion purposes. This may include journals/books published, research papers, proof of seminars conducted/facilitated/attended, and the like.

6.9.2.5. Foreign Employees will be asked to submit personal documents such as passport and visa so that the School can assist them in acquiring proper work permits.

**6.9.3. Health Maintenance Organization and Annual Physical Examination**

6.9.3.1. Full-time Employees/Personnel are automatically enrolled in the School's chosen Health Maintenance Organization (HMO). Part-time faculty have an option to enroll. Employees/Personnel who enroll their dependents will be required to fill out an enrollment form and provide personal information of the dependent. All employees and their dependents who avail of the HMO are required to sign an HMO Consent and Waiver Form.

6.9.3.2. All regular employees are required to participate in an Annual Physical Exam. The diagnostics laboratory will send and share the medical results with the School Clinic. The results may include, but are not limited to, physical exam, complete blood count, chest x-ray, drug test, electrocardiogram, and pap smear.

**6.9.4. Leave Benefits**

Employees/Personnel are required to provide essential information and medical documents when necessary for filing of leave benefits (Emergency leave, Sick Leave, Vacation/Service Leave, Solo Parent Leave, Special Leave Without Pay, Sabbatical Leave, Birthday Leave).

**6.9.5. Community Support**

The employees/personnel may voluntarily provide necessary information such as medical condition, bank account information and mobile wallet application account which will be shared to the community should they prefer to solicit community support.

**6.9.6. Local and International Travel**

Employees/personnel may be asked to provide personal documents such as passport, visa, medical clearance and the like when they join a school activity or get endorsement from the School to participate in an activity that involves travelling.

**6.9.7. Study Grant and Study Leave**

Employees/personnel who would like to apply for benefits (study grant, study leave, Brother President Scholarship grant, training, etc.) will be asked to fill out a form which may include pertinent personal information needed for performance school verification and approval.

**6.9.8. Performance Evaluation**

Employees/Personnel are regularly evaluated by their supervisors, peers and their clients (faculty are evaluated by students) and the results are kept on file.

**6.9.9. School Services and Activities**

While working for the School, the employee/personnel may be asked for some of his or her personal information to access services in the School (for example: Learning Resource Center, Finance Resource Department, Health Service Unit, laboratories, etc.)

The employee/personnel may also be asked for some personal information to be involved in certain activities of the School (for example: retreats, seminars, workshops, social action, exchange program, formation sessions, etc.)

**6.9.10. Grievance and Disciplinary Cases**

HRDO keeps track of grievances and on-going disciplinary cases against faculty and personnel. Incident Reports and case decisions are kept on file and shall only be shared with authorized persons/offices on a need to know basis.

**6.9.11. Retirement**

Upon resignation or retirement (mandatory or voluntary), employee/personnel will either submit a resignation letter or file and sign a retirement application including exit interview form, Waiver and Quitclaim and Release

**6.10. Transparency, Legitimate Purpose, and Proportionality**

- 6.10.1. Personal data collected shall be processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.
- 6.10.1.1. **Transparency.** The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal information, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal information should be easy to access and understand, using clear and plain language.  
The processor is required to provide detailed, specific information to data subjects whether the information was collected directly from data subjects or indirectly from other sources. The data subject must be informed through an appropriate privacy notice.
- 6.10.1.2. **Legitimate Purpose.** The processing of information shall be compatible with a declared and specified purpose. It must not be contrary to law, morals, or public policy.  
Personal data must not be further processed in any manner incompatible with the original purpose/s. If the personal information will be used for a new, different or incompatible purpose, the data subject needs to give his/her consent.
- 6.10.1.3. **Proportionality.** The processing of personal data shall be adequate, relevant, suitable and necessary in relation to the purposes for which it is processed. It should not be excessive. Large volumes of personal data not relevant to purposes for which they were intended to be processed should not be collected.
- 6.10.1.4. All processors or users of personal data within LSGH shall only process the information fairly, lawfully and for specified purposes. These restrictions are not intended to prevent processing, but to ensure that LSGH processes personal information for legitimate purposes without prejudicing data subject rights.

## 6.11. Lawful Processing

- 6.11.1. Lawful processing of personal information can be any of the following:
- 6.11.1.1. Data subject has given his or her consent prior to the collection, or as soon as practicable and reasonable; if data subject is below 18 years old, his parent or legal guardian as provided in his school records shall be his representative;
- 6.11.1.2. The processing is required due to a contract;
- 6.11.1.3. It is necessary due to a legal obligation;
- 6.11.1.4. The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;
- 6.11.1.5. The processing is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law; and
- 6.11.1.6. The processing is necessary to pursue the legitimate interests of LSGH, or by a third party to whom the personal information is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject under the Philippine Constitution.
- 6.11.2. Lawful processing of sensitive personal information or privileged information can be any of the following:
- 6.11.2.1. Data subject has given his or her consent prior to the processing; if data subject is below 18 years old, his parent or legal guardian as provided in his school records shall be his representative;
- 6.11.2.2. The processing is provided for by existing laws and regulation, provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;
- 6.11.2.3. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
- 6.11.2.4. The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations provided that:
- 6.11.2.5. Processing is confined and related to the bona fide members of these organizations or their associations;
- 6.11.2.6. The information is not transferred to third parties; and

- 6.11.2.7. Consent of the data subject was obtained prior to processing.
- 6.11.2.8. The processing is necessary for the purpose of medical treatment: Provided that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured.
- 6.11.2.9. The processing of the information is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

6.12. **Data Privacy Security Awareness, Education and Training**

All Students, Parents, Guardian, Alumni/Alumnae and Employees/Personnel shall be adequately trained in Data Privacy security procedures and the correct use of Information Technology facilities.

6.13. **Security Measures for Protection of Personal Information**

6.13.1. **Organizational Measure**

- 6.13.1.1. The School shall conduct a regular Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data.
- 6.13.1.2. LSGH shall appoint a Data Protection Officer and such appointment shall be registered with the National Privacy Commission
- 6.13.1.3. LSGH shall adopt the Privacy by Design (PbD) Framework in processing personal data.
- 6.13.1.4. LSGH shall develop a Privacy Management Plan.
- 6.13.1.5. Each office, department and unit shall accomplish a Privacy Data Inventory, Privacy Impact Assessment and Privacy Risk Map for each of their process, project, system or technology that processes personal data (new or existing).
- 6.13.1.6. All heads of departments are responsible for ensuring that all employees/personnel within their area of responsibility, comply with this policy and should develop their own data privacy guidelines to implement appropriate practices, processes and controls and training to ensure compliance within their offices/units/ departments.
- 6.13.1.7. LSGH shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.
- 6.13.1.8. All employees will be asked to sign a Confidentiality and Non-Disclosure Agreement.
- 6.13.1.9. All employees with access to personal information shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.
- 6.13.1.10. Data privacy protection shall be part of an employee's term and conditions of employment, breach of data privacy policy due to unauthorized access misuse or loss may result in disciplinary action up to and including dismissal. This obligation shall continue even after transferring to another position, or upon terminating their employment or contractual relations.
- 6.13.1.11. LSGH through the Risk Management Compliance Office shall provide capacity building, orientation or training programs personnel regarding privacy or security policies. There shall be mandatory training on data privacy and security at least once a year for personnel directly involved in the processing of personal data. Their heads of departments/units shall ensure their attendance and participation in relevant training and orientations regularly.
- 6.13.1.12. The Risk Management Compliance Office will do periodic audits to ensure compliance with this policy and the DPA.
- 6.13.1.13. LSGH through appropriate contractual agreements, shall ensure that its Personal Information Processors (PIP), where applicable, shall also implement the security measures required by the DPA and its implementing rules and regulations (IRR). It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified by the DPA and its IRR, and ensure the protection of the rights of the data subject.

- 6.13.1.14. Usage of school issued devices shall be restricted to official business purposes. Personnel must be aware and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.
- 6.13.1.15. Off-site computer usage, whether at home or at other locations, may only be used with the authorization from the office/department Head.
- 6.13.1.16. Personnel who are issued with portable computers and who intend to travel for work purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimize the risks.
- 6.13.1.17. Due to the nature of the device being mobile and that at times it is outside the protected premises of the school, the custodian must take care of all information on the device as well as prevent unauthorized personnel from accessing the information on the device.
  - 6.13.1.17.1. Personnel are prohibited from tampering or making any modification or changes to the device's technical specifications. Should there be a need for upgrade, the personnel should coordinate with the TMC for assessment and approval.
  - 6.13.1.17.2. Personnel are prohibited to install any unauthorized, unlicensed or pirated software/applications in the device. Unauthorized software refers to software not allowed by the school regardless of its license status.
- 6.13.1.18. To ensure availability of software upon release of the device, HRDO will coordinate with the immediate heads and/or directors regarding the required software of specific personnel items. Should there be a need to install a particular software or application needed for classroom instruction and/or work-related tasks, the personnel should raise a request, only upon endorsement of the immediate supervisor, through TMC for assessment and approval.
- 6.13.1.19. Devices are not to be used to make sound recordings without the consent of all persons being recorded. Recordings must be disposed of based on LSGH data retention and disposal guidelines.
- 6.13.1.20. It is the sole responsibility of the custodian to back-up their own data. Back-up methods include storage in cloud-based services. Backups on external storage shall be allowed on school issued storage devices.
- 6.13.1.21. TMC shall ensure that issued devices are updated with softwares such as anti-virus, anti-malware and the like.
- 6.13.1.22. The school shall have the right to monitor the use of issued devices using a variety of methods to ensure compliance with school policies. Deletion and tampering of system logs is prohibited.
- 6.13.1.23. Issued devices remain to be a school property and are considered a fixed asset. The personnel assigned these devices shall be considered as the custodian of the device.
- 6.13.1.24. If the device is returned by the custodian, TMC shall manage/clean the device before it becomes part of the pool for distribution to other eligible personnel in the program.

#### **6.13.2. Physical Security Measures**

- 6.13.2.1. Personal data in the custody of the School may be in digital/electronic format and paper-based/physical format.
- 6.13.2.2. All personal data processed by the School shall be stored in the office/department who owns the data. Paper based documents shall be kept in a locked filing cabinet while the digital/electronic files stored in computers/servers provided and installed by the School shall be secured by password/s and digital devices should be turned off, locked and stored carefully when not in use.
- 6.13.2.3. Only authorized personnel shall be allowed to have access to personal data stored in offices/departments. Other personnel may be granted access upon filing of an access request form with the Office/Department Head and the latter's approval thereof.
- 6.13.2.4. All employees/personnel shall not be allowed to take out physical files from the office except for a legitimate purpose and with written permission from the Office/department Head.
- 6.13.2.5. All employees/personnel authorized to access the data must register with the online registration platform or access logbook. They

- 6.13.2.6. shall indicate the date, time, duration, and purpose of the access. Computers shall be positioned with considerable spaces between them to maintain and protect the processing of personal data. If in a work from home set-up, the personnel shall create workspaces in private areas and make sure that unauthorized or accidental viewing by others is avoided.
- 6.13.2.7. The School's work areas chosen to locate computers and to store data shall be suitably protected from physical intrusion, theft, fire, flood and other hazards.
- 6.13.2.8. The School's premises shall be safeguarded against unlawful and unauthorized physical intrusion.
- 6.13.2.9. When moving and deploying computers and other hardware, suitable precautions shall be taken to guard against the environmental threats of fire, flood and excessive ambient temperature / humidity.
- 6.13.2.10. All the School's premises shall be protected from unauthorized access using ID cards and security cameras to monitor movements.
- 6.13.2.11. Secure areas are set up and designed in a way suitable to protect the sensitive and critical information and/or assets being safeguarded.
- 6.13.2.12. Access to delivery and loading areas and other similar areas shall be restricted to identified and authorized personnel.

**6.13.3. Technical Measures**

- 6.13.3.1. The School shall implement technical security measures to make sure that there are 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.
- 6.13.3.2. Where appropriate LSGH shall adopt the following measures:
  - 6.13.3.2.1. Info Security, IT Security and Infonet Policy with respect to the processing of personal data;
  - 6.13.3.2.2. Design and implement safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;
  - 6.13.3.2.3. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;
  - 6.13.3.2.4. Regular monitoring for security incidents/breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;
  - 6.13.3.2.5. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - 6.13.3.2.6. A process for regularly penetration testing, assessing, and evaluating the effectiveness of security measures;
  - 6.13.3.2.7. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.
  - 6.13.3.2.8. School issued devices are protected by security settings and features adopted by the school. At the minimum, personnel should not disclose school credentials and passwords to unauthorized individuals.
  - 6.13.3.2.9. Information and data stored on laptop or portable computers must be backed up regularly in a secure device. It is the responsibility of the user to ensure that this takes place on a regular basis.

**6.13.4. Email Use**

**6.13.4.1. Student Email Account**

- 6.13.4.1.1. The student email account should be used for education and school student affairs only.
- 6.13.4.1.2. The email system shall not be used for the creation or

distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair, color, disabilities, age, sexual orientation, pornography, religious beliefs and practices, political beliefs, or national origin. Students, Parents/Guardians and Alumni who receive any emails with this content from any member of the LSGH community should report the matter to the Technology Management Center (TMC).

- 6.13.4.1.3. Using a reasonable amount of resources for personal emails by Students is acceptable, but non-school related email shall be saved in a separate folder from school related email. Sending chain letters, joke emails and the like is prohibited.
- 6.13.4.1.4. Virus or other malware warnings and mass mailings shall be reported by the TMC before sending. These restrictions apply to the forwarding of mail received by a Student, Parent/Guardian or Alumni.
- 6.13.4.1.5. Students shall have no expectation of privacy in anything they store, send or receive on the School's email system. The School's TMC may monitor messages without prior notice. However, the TMC is not obliged to monitor email messages.
- 6.13.4.1.6. Students must exercise utmost caution when sending any email from inside to an outside network.
- 6.13.4.1.7. Upon graduation or change of school, the student email account shall be deactivated.
- 6.13.4.1.8. Email communication by students should contain an LSGH email disclaimer.
- 6.13.4.2. **Employees/Personnel Email Account**
  - 6.13.4.2.1. The email should be used for work communications and transactions only.
  - 6.13.4.2.2. The email system shall not be used for the creation or distribution of any disruptive or offensive messages, including but not limited to offensive comments about race, gender, color, disabilities, age, sexual orientation, religious beliefs and practices, political beliefs, or national origin. Employees who receive any emails with this content from any employees should report the matter to TMC immediately.
  - 6.13.4.2.3. Using a reasonable amount of resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke e-mails is prohibited.
  - 6.13.4.2.4. Virus or other malware warnings and mass mailings shall be reported by the TMC before sending. These restrictions apply to the forwarding of mail received by an employee/personnel.
  - 6.13.4.2.5. All employees/personnel shall have no expectation of privacy in anything they store, send or receive on the company's email system. The School's TMC may monitor messages without prior notice. However, the Technology Management Center is not obliged to monitor email messages.
  - 6.13.4.2.6. Employees must exercise utmost caution when sending any email most especially sending emails from inside to an outside network. Email addressees should be double checked.
  - 6.13.4.2.7. Email communication by employees should contain a LSGH email disclaimer.
- 6.13.5. **Data Protection Officer (DPO)**
  - 6.13.5.1. The school shall designate a Data Protection Officer.
  - 6.13.5.2. Functions of the DPO or any other responsible personnel with similar functions.
  - 6.13.5.3. The Data Protection Officer shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol and the inquiry and complaints procedure.

**6.13.6. Review of Data Privacy**

- 6.13.6.1. This Policy shall be reviewed and evaluated once every two (2) years. Privacy and security policies and practices within the School shall be updated to remain consistent with the current data privacy best practices.
- 6.13.6.2. Recording and documentation of activities carried out by the DPO, or the School itself to ensure compliance with the DPA, IRR and other relevant policies.
- 6.13.6.3. There shall be a detailed and accurate documentation of all activities, projects and processing systems of the School, to be carried out by the Data Protection Officer.

**6.13.7. Incident Management**

- 6.13.7.1. The Data Protection Officer shall oversee the compliance of the School with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol and the inquiry and complaints procedure.
- 6.13.7.2. All security incidents shall be reported through the Data Protection Officer and Data Breach Response Team immediately upon the discovery of the incident. This shall be followed by a written incident report.
- 6.13.7.3. All access logs containing the username, time of access, duration of use for all users who access the network shall be kept and shall be provided to management or authorized governmental authorities in case of any official investigations.
- 6.13.7.4. Incident Response Process applies to any unlawful, unauthorized or any unacceptable action that involves a computer system or computer network within the School. Examples of such security incidents, includes but is not limited to the following:
  - 6.13.7.4.1. Computer virus or worm outbreak;
  - 6.13.7.4.2. Theft of trade secrets;
  - 6.13.7.4.3. Unauthorized disclosure or access to confidential information/personal data;
  - 6.13.7.4.4. Email spam or harassment;
  - 6.13.7.4.5. Unauthorized or unlawful intrusion into computing systems;
  - 6.13.7.4.6. Embezzlement;
  - 6.13.7.4.7. Denial of service (DOS) attacks;
  - 6.13.7.4.8. Extortion; and
  - 6.13.7.4.9. Any unlawful action where the evidence of such action may be stored on computer media such as fraud, threats, and traditional crimes.

**6.13.8. Monitoring for Security Breaches**

The School shall use an intrusion cybersecurity detection system to monitor security breaches and alert the School of any attempt to interrupt or disturb the system.

**6.13.9. Security Features of the Software/s and Application/s Used**

- 6.13.9.1. The School shall first review and evaluate software application before the installation thereof in computers and devices of the School to ensure the compatibility of security features with overall operations.
- 6.13.9.2. The School shall do regular testing, assessment and evaluation of effectiveness of security measures
- 6.13.9.3. The School shall review security facilities, conduct vulnerability assessments and perform penetration testing within the School on a regular schedule to be prescribed by the Technology Management Center (TMC).
- 6.13.9.4. The School shall apply encryption, authentication process, and other technical security measures that control and limit access to personal data
- 6.13.9.5. Each personnel with access to personal data shall verify his or her identity using an encrypted link and multi-level authentication.

**6.13.10. Breach and Security Incidents**

The School shall develop and implement policies and procedures for the management of a personal data breach, including security incidents.

**6.13.11. Creation of Data Breach Response Team**

- 6.13.11.1. A Data Breach Response Team of at least five (5) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effect of the breach.
- 6.13.11.2. The Data Breach Response Team is composed of the following:
  - 6.13.11.2.1. Director of Administration - to ensure management's commitment to breach response planning and execution
  - 6.13.11.2.2. Head Administrator of Marketing Communication Office - to ensure an accurate account of any issues is communicated to stakeholders and the press
  - 6.13.11.2.3. Data Protection Officer - to ensure that any evidence collected maintains its value in the event that the company chooses to take legal action and also provide advice regarding liability issues when an incident affects data subjects and/or the general public
  - 6.13.11.2.4. Head Administrator of TMC - to work directly with the affected network to research the time, location, and details of a breach
  - 6.13.11.2.5. Head Administrator of the Source of Breach - to ensure that there is cooperation in the investigation and securing evidence in his office, department or unit.
  - 6.13.11.2.6. Head Administrator of Safety and Security Office - to conduct investigation in cases of physical break-in.

**6.13.12. Measures to Prevent and Minimize Occurrence of Breach and Security Incidents**

The School shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend training and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the School.

**6.13.13. Disciplinary Process for Breach of Security**

Any violation of School Data Privacy and information security policies shall be appropriately dealt with through a formal disciplinary process as provided in the IOM or Student Formation Handbook.

**6.13.14. Privacy Notices**

LSGH and all departments and units processing personal data must provide data subjects with a privacy notice to inform them how and for what purpose their personal data is processed. These notices may be in the form of general privacy statements applicable to specific groups of individuals or may be stand alone, one-time privacy statements covering processing related to a specific purpose. A template and guidance for privacy notices are found in the Annex "A" of this policy.

**6.13.15. Data Retention and Disposal Procedure**

- 6.13.15.1. The School shall retain personal data in accordance with its data retention policy. Upon expiration of the set periods, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.
- 6.13.15.2. Personal information must not be kept longer than necessary for the purposes for which it was originally collected. This applies to all personal information, whether held on core systems, local PCs, laptops or mobile devices or held on paper.
- 6.13.15.3. If the data is no longer required, it must be securely disposed by shredding or by deletion.
- 6.13.15.4. The office, department or unit must set its own retention schedules based on legal and business requirements or based on industry practice.

**6.13.16. Privacy by Design Framework (PbD)**

- 6.13.16.1. By applying PbD framework LSGH shall:
  - 6.13.16.1.1. Take a proactive rather than a reactive measure. It anticipates the risks and prevents privacy incidents before they occur.



- 6.13.16.1.2. Seek to deliver the maximum degree of privacy by ensuring personal information is automatically protected as a practice. No action on the part of the individual is needed in order to protect their privacy.
- 6.13.16.1.3. Embed PbD into the design and architecture of the IT system and business practices of LSGH. Privacy shall be integrated into the system without diminishing LSGH's functions.
- 6.13.16.1.4. Seek to accommodate all legitimate objectives in a positive-sum "win-win" manner
- 6.13.16.1.5. Embed PbD into the system prior to the first element of information being collected and extends securely throughout the entire lifecycle of the data involved.
- 6.13.16.1.6. Seek to assure all stakeholders that whatever the business practice and technology involved is operating in accordance to the objectives of this policy
- 6.13.16.1.7. Require architects and operators to keep the interests of the individual primary by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.
- 6.13.16.1.8. Require each department or unit to implement Privacy by Design measures when processing personal information, by implementing appropriate technical and organizational measures in an effective manner, to ensure compliance with data-protection principles. To further reduce the risks associated with handling personal information, whenever possible anonymization should be applied, if not possible, pseudonymization.
- 6.13.16.1.9. Ensure that data-handling practices default to privacy, in order to minimize unwarranted intrusions in privacy (e.g. by disseminating personal information to those who need to receive it to discharge their duties). Personal information should not be available to an indefinite number of persons.

**6.13.17. Personal Data Inventory** (can be found here as Annex "C")

- 6.13.17.1. Each department or unit shall regularly accomplish/update the Personal Data Inventory (PDI). This is needed to be able to adopt a meaningful privacy management program to comply with the law. The PDI includes the following:
  - 6.13.17.1.1. Personal data collected and processed;
  - 6.13.17.1.2. Purpose of the collection/processing of the personal data;
  - 6.13.17.1.3. Owner of the personal data;
  - 6.13.17.1.4. Legal basis of the collection/processing;
  - 6.13.17.1.5. Storage location of data including third party systems and where their servers are located;
  - 6.13.17.1.6. Mapping where the data goes from point of collection internally and externally;
  - 6.13.17.1.7. Access control to data (read only or can edit)
  - 6.13.17.1.8. Existing policies if there are any on use, disclosure, protection, back-up and disposal policies Period of retention of data and format of data

**6.13.18. Privacy Impact Assessment**

- 6.13.18.1. When considering new processing activities or setting up new procedures or systems that involve personal information, the office, department or unit must always consider privacy issues at the earliest stage and Privacy Impact Assessment (PIA) must be conducted. The PIA is a mechanism to identify and examine the impact of new initiatives and put in place measures to minimize or reduce risks during the design stages of a process and throughout the life cycle of the initiative. This includes implementing appropriate technical and organizational measures to minimize the potential negative processing can have on the data subjects' privacy. This will ensure that privacy and data protection control requirements are not an afterthought. A template and guidance for PIA can be found here as Annex "C".
- 6.13.18.2. A PIA should be conducted in the following cases:
  - 6.13.18.2.1. the use of new technologies or changing technologies (programs, systems or processes);
  - 6.13.18.2.2. automated processing including profiling;
  - 6.13.18.2.3. large scale processing of sensitive data;

- 6.13.18.2.4. large scale and systematic monitoring of publicly accessible areas(e.g. CCTV)
- 6.13.18.3. A PIA must include:
  - 6.13.18.3.1. Description of the program, project, process, measure, system or technology and including expected benefits which requires the collection of personal information;
  - 6.13.18.3.2. Description of the information lifecycle including personal information data process flow;
  - 6.13.18.3.3. Description of legal grounds for processing personal information including copies of forms used (e.g. consent forms); and
  - 6.13.18.3.4. Identification of the privacy risks and type of risks.

**6.13.19. Risk Map**

- 6.13.19.1. A Risk Map is an assessment of the severity and likelihood of identified risks.
- 6.13.19.2. It includes a list of proposed controls with type (organizational, physical, or technical), estimated cost, and estimated implementation timeframe

**6.13.20. Hiring Third Party Processors or Personal Information Processors (PIP)**

- 6.13.20.1. Where external processors are hired to process personal information on behalf of LSGH:
  - 6.13.20.1.1. Personal Information Processor (PIP) must be chosen by LSGH which provide sufficient guarantees about security measures to protect the processing of personal data;
  - 6.13.20.1.2. LSGH must take reasonable steps that security measures are in place; and
  - 6.13.20.1.3. There should be a written contract (a data processing agreement) establishing what personal information will be processed and for what purpose, signed by LSGH and the PIP.

**6.13.21. Processing of Personal Information/Data for Research**

- 6.13.21.1. Before researchers can process, collect and/or use any personal data as part of a research project, an appropriate legal basis for the processing of the data must be identified. It can be one of the following:
  - 6.13.21.1.1. Informed and freely given consent, public interest, legitimate or contract
  - 6.13.21.1.2. Research subject's/participants' data privacy shall be protected. This includes but are not limited to the following:
    - 6.13.21.1.2.1. The research subjects must be aware how their data will be used and may object if they wish;
    - 6.13.21.1.2.2. Personal data should be kept confidential and can only be shared with research subject's permission;
    - 6.13.21.1.2.3. There should be no substantial damage or distress to research subjects;
    - 6.13.21.1.2.4. There should be data minimization. The processing of personal data should just be sufficient to fulfill the research purpose and should be relevant and limited to what is necessary;
    - 6.13.21.1.2.5. There should be anonymizing or pseudonymization of data whenever possible;
    - 6.13.21.1.2.6. Ensure the personal information is kept secured and only accessed by those authorized to do so.

**6.14. Data Subject Rights**

- 6.14.1. The DPA contain eight (8) data subject rights to which LSGH must comply with:

**6.14.1.1. Right to be informed**

- 6.14.1.1.1. This applies whether personal information pertaining to the data subject shall be, are being, or have been processed. It includes any form of automated processing of personal information consisting of use of personal data.
- 6.14.1.1.2. Data subject is notified and furnished of the following before the entry of data subject's personal information into the processing system of LSGH as personal information controller, or at the next practical opportunity:

- 6.14.1.1.2.1. Description of the personal data to be entered into the system;
- 6.14.1.1.2.2. Purposes for which information are being processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
- 6.14.1.1.2.3. Basis of processing, when processing is not based on the consent of the data subject;
- 6.14.1.1.2.4. Scope and method of the personal information processing;
- 6.14.1.1.2.5. The recipients of the personal information or to whom it may be disclosed;
- 6.14.1.1.2.6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
- 6.14.1.1.2.7. The identity and contact details of the personal information controller or its Data Protection Officer (DPO);
- 6.14.1.1.2.8. The period for which the information will be stored; and
- 6.14.1.1.2.9. The existence of their rights as data subjects

6.14.1.2. **Right to Object**

- 6.14.1.2.1. The data subject shall have the right to object to the processing of his or her personal information, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject.
- 6.14.1.2.2. When a data subject objects or withholds consent, the processor shall no longer process the personal data, unless:
  - 6.14.1.2.2.1. The personal data is needed pursuant to a subpoena;
  - 6.14.1.2.2.2. The collection and processing are for obvious, legitimate purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
  - 6.14.1.2.2.3. The information is being collected and processed as a result of legal obligation.

6.14.1.3. **Right to Access.**

- 6.14.1.3.1. The data subject has the right to reasonable access to, upon demand, the following:
  - 6.14.1.3.1.1. Contents of personal information of the data subject that were processed;
  - 6.14.1.3.1.2. Sources from which personal data were obtained;
  - 6.14.1.3.1.3. Names and addresses of recipients of the personal information;
  - 6.14.1.3.1.4. Manner by which such data were processed
  - 6.14.1.3.1.5. Reasons for the disclosure of the personal information to recipients, if any;
  - 6.14.1.3.1.6. Information on automated processes where the information will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
  - 6.14.1.3.1.7. Date when his or her personal data concerning the data subject were last accessed and modified;
  - 6.14.1.3.1.8. Until how long will his or her personal data be retained and the manner it will be disposed of
  - 6.14.1.3.1.9. The designation, name or identity, and address of the personal information controller.

6.14.1.4. **Right to Rectification/Correction**

- 6.14.1.4.1. The data subject has the right to dispute the inaccuracy or error in the personal information and have LSGH correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.

- 6.14.1.4.2. If the personal information has been corrected, LSGH shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof. The recipients or 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.
- 6.14.1.5. **Right to Erasure or Blocking**
  - 6.14.1.5.1. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal information from LSGH's filing system. This right may be exercised upon discovery and substantial proof of any of the following:
    - 6.14.1.5.1.1. The personal information is incomplete, outdated, false, or unlawfully obtained;
    - 6.14.1.5.1.2. The personal information is being used for purpose not authorized by the data subject;
    - 6.14.1.5.1.3. The personal information is no longer necessary for the purposes for which they were collected;
    - 6.14.1.5.1.4. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
    - 6.14.1.5.1.5. The personal information concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
    - 6.14.1.5.1.6. The processing is unlawful;
    - 6.14.1.5.1.7. The processor violated the rights of the data subject;
    - 6.14.1.5.1.8. In some circumstances, data subjects may not wish to have their personal information erased but rather have any further processing restricted. In limited situations, data subjects may object to further processing of their personal information.
  - 6.14.1.5.2. In some circumstances, if personal data are incomplete, the data subject can also require LSGH to complete the data or to record a supplementary statement.
- 6.14.1.6. **Right to Data Portability**

Where the personal information is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from LSGH a copy of such information in an electronic or structured format that is commonly used and allows for further use by the data subject.
- 6.14.1.7. **Right to Damages**

The data subject may be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information, taking into account any violation of his or her rights and freedom as data subject.
- 6.14.1.8. **Right to File a Complaint**
  - 6.14.1.8.1. Data subjects have the right to file a complaint. LSGH through the DPO must respond to these requests within thirty (30) days. It is an offense to delete relevant personal information after the data subject's access request has been received.
  - 6.14.1.8.2. The lawful heirs and assigns of the data subject (e.g. parent of student) may invoke the rights of the data subject to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising his or her data subject rights.
  - 6.14.1.8.3. Where the legal basis of processing is consent the data subject may withdraw such consent. However, the data subject needs to demonstrate valid and reasonable grounds for withdrawal relating to their particular situation.
  - 6.14.1.8.4. Data subjects have the right to object to specific types of

processing such as processing for direct marketing, research or statistical purposes. The data subject needs to present valid and reasonable grounds for objecting to the processing relating to their particular situation except in direct marketing where it is an absolute right. Individuals receiving these kinds of requests should not act to respond but instead contact the Data Protection Officer immediately.

**6.14.2. Rights in Relation to Automated Decision Making and Profiling**

In case of automated decision making and profiling that may have significant effects on data subjects, they have the right to either have the decision reviewed by a human being or not to be subjected to this type of decision making at all. These requests must be forwarded to the Data Protection Officer immediately.

**6.15. Record Keeping**

6.15.1. LSGH shall keep full and accurate records of all its data processing activities. Offices, departments or units must keep and maintain accurate records reflecting LSGH's processing, including records of data subjects' consents and procedures for obtaining consents, where consent is the legal basis of processing

6.15.2. These records should include, at a minimum, the name and contact details of LSGH as Personal Information Controller (PIC) and of the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place

6.15.3. Records of personal data breaches must also be kept, setting out:

- 6.15.3.1. Facts surrounding the breach
- 6.15.3.2. Effects of the data breach; and
- 6.15.3.3. Remedial action taken

**6.16. Access**

6.16.1. Due to the confidential and at times sensitive nature of the personal data under the custody of LSGH, only school officials who have a legitimate educational interest/legitimate interest have access to these records.

6.16.2. A school official is:

- 6.16.2.1. A person employed by LSGH in an administrative, supervisory, academic or research, security services, or support staff position, including health or medical staff and also clerical staff who have access to the student/personnel record;
- 6.16.2.2. A contractor, consultant, volunteer or other service provider with whom LSGH has contracted as its agent to provide a service that would otherwise be performed by a LSGH employee, such as (but not limited to) an attorney, auditor, healthcare provider and security agency;
- 6.16.2.3. An individual serving on an official committee, such as a disciplinary or grievance committee, or who is assisting another school official in performing his/her tasks; and
- 6.16.2.4. An individual serving in the Board of Trustees.

6.16.3. A school official has a legitimate educational interest/legitimate interest if the official is:

- 6.16.3.1. Performing a task that is specified in his/her position description or contract agreement;
- 6.16.3.2. Performing a task related to the discipline of a student/employee;
- 6.16.3.3. Providing a service or benefit relating to the student or student's family or employee or employee's family, such as health care, counselling, job placement, or financial aid discipline cases and;
- 6.16.3.4. Maintaining the safety and security of the campus.

**6.17. Data Sharing**

6.17.1. Student/Employee personal information is shared internally within LSGH when appropriate to meet legitimate purposes. Data will only be shared between employees who have the official need to have access to it. All employees of LSGH shall maintain confidentiality of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations.

6.17.2. When personal information is transferred internally, the recipient must only process the information in a manner consistent with the original purpose for

which the data is collected.

- 6.17.3. If personal information is shared internally for a new and different purpose, a new privacy notice should be provided to the data subject and if necessary acquire data subject's consent.
- 6.17.4. When personal information is transferred externally, a legal basis must be determined and data sharing agreement/service legal agreement between LSGH and the third party must be signed, unless disclosure is required by law, such as DepEd, Bureau of Internal Revenue, and Department of Labor and Employment.
- 6.17.5. If transferring personal information outside the Philippines, personnel involved in transferring personal information must inform the DPO first to ensure that appropriate safeguards are in place before agreeing to any such transfer. Personal information can be transferred in the following cases:
  - 6.17.5.1. Data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
  - 6.17.5.2. The transfer is necessary for one of the other reasons set out in the EU General Data Protection Regulation (GDPR) including:
    - 6.17.5.2.1. The performance of a contract between LSGH and the data subject (e.g. student exchange program);
    - 6.17.5.2.2. Reasons of public interest;
    - 6.17.5.2.3. To establish, exercise or defend legal claims; or
    - 6.17.5.2.4. To protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.
  - 6.17.5.3. LSGH has a full range of standard transfer agreements and clauses and the data subject should seek guidance from the DPO at [dpo@lsg.edu.ph](mailto:dpo@lsg.edu.ph) before any transfer of personal data takes place.

#### 6.18. **Disclosure**

- 6.18.1. Personal data under the custody of LSGH shall be disclosed only pursuant to a lawful purpose, and to authorize recipients of such data. Personal information shall always be held securely and shall not be disclosed to any unauthorized third party either accidentally, negligently or intentionally.
- 6.18.2. In the absence of consent, a legal obligation or other legal basis of processing, personal information should not generally be disclosed to third parties unrelated to LSGH (e.g. students' parents, members of the public, private property owners). If a student is 18 years old and above, the students' parent/s and/or guardians do not have an automatic right to gain access to their child's data unless their child has signed the consent form allowing them access to his/ her records.
- 6.18.3. Some government agencies have a statutory power to obtain information. Employees or students should seek confirmation of any such power before disclosing personal data in response to a request. If the data subject needs guidance, he/ she should contact the DPO.
- 6.18.4. Without a search warrant subpoena, the law enforcement officers have no automatic right of access to records of personal information, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. In such cases, the law enforcement officers may contact the DPO for guidance.

#### 6.19. **Direct Marketing**

- 6.19.1. Direct Marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For LSGH, this will include notification about events, fundraising, selling of goods or services. Marketing covers all, such as contact by mail, telephone and electronic messages (emails and text messaging). The LSGH must ensure that it complies with relevant legislations when it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

#### 6.20. **Responsibilities of DPO, LSGH, Students and Employees**

##### 6.20.1. **Responsibilities of the Data Protection Officer**

- 6.20.1.1. 5.24.1 The DPO shall in the performance of his/her tasks, have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing
- 6.20.1.2. The DPO is responsible for:
  - 6.20.1.2.1. Advise LSGH and the community (personnel and students) of its obligation under the DPA;

- 6.20.1.2.2. Monitor compliance with the DPA, IRR, other relevant legislations and regulations, LSGH's policies on data protection and monitoring and training and audit activities related to data privacy;
  - 6.20.1.2.3. Provide advice where requested on data privacy concerns; and
  - 6.20.1.2.4. Cooperate with and act as the point of contact for the NPC.
- 6.20.2. **Responsibilities of LSGH**  
As the Personal Information Controller (PIC), LSGH is responsible for establishing policies and procedures in order to comply with the DPA and other relevant legislations and regulations.
- 6.20.3. **Responsibilities of Students and Employees/Personnel Processing Personal Information**
- 6.20.3.1. Students and Employees/Personnel processing personal information shall ensure that:
    - 6.20.3.1.1. All personal information is kept securely;
    - 6.20.3.1.2. No personal information is disclosed either verbally, in writing or electronically, accidentally or otherwise, to any unauthorized third party;
    - 6.20.3.1.3. Personal information is kept in accordance with LSGH's retention schedule;
    - 6.20.3.1.4. Any queries regarding data protection, including data subject's access requests and complaints, are promptly directed to the Data Protection Officer;
    - 6.20.3.1.5. Any data protection incidents are swiftly brought to the attention of the Data Protection Officer and support in resolving breaches;
    - 6.20.3.1.6. Where there is doubt or uncertainty around a data protection concern, advice should be sought from the Data Protection Officer;
    - 6.20.3.1.7. Where personnel are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the data protection principles.
    - 6.20.3.1.8. Personnel who are unsure about who are the authorized third parties to whom they can legitimately disclose personal data should seek advice from the Data Protection Officer.
  - 6.20.3.2. Heads of office, departments or units who employ contractors, short term or voluntary staff shall:
    - 6.20.3.2.1. Ensure contractors, short term or voluntary staff sign a Confidentiality and Non-Disclosure Agreement;
    - 6.20.3.2.2. Take all practical and reasonable steps to ensure that contractors, short term or voluntary staff do not have access to any personal information beyond what is essential for the work to be carried out properly;
    - 6.20.3.2.3. Appropriately appraise Contractors, Short Term or Voluntary Staff for the data they will be processing;
    - 6.20.3.2.4. Ensure that Contractors, Short Term or Voluntary Staff comply with the following:
      - 6.20.3.2.4.1. Keep secure and confidential any personal data collected or processed in the course of work undertaken for LSGH;
      - 6.20.3.2.4.2. Return to LSGH all personal data upon completion of the work, including any copies that may have been made;
      - 6.20.3.2.4.3. Notify LSGH of any disclosure of personal information to any other organization or any person who is not a direct employee of the contractor; and
      - 6.20.3.2.4.4. Not to store nor process any personal data made available by LSGH, or collected in the course of work outside the Philippines, unless a written consent to do so has been received by LSGH.
- 6.20.4. **Responsibilities of Students and Employees/Personnel**
- 6.20.4.1. **Students and Employees are responsible for:**
    - 6.20.4.1.1. Familiarizing themselves with the Privacy Notice provided when they register with LSGH:

- 6.20.4.1.1.1. Ensuring that the personal information they provided to LSGH are accurate and up to date;
- 6.20.4.1.1.2. Reporting Breach and/or Security Incidents.
- 6.20.4.1.1.3. Abiding with LSGH policies and procedures for the management of a personal data breach, including incidents

**6.21. Creation of Data Breach Response Team**

- 6.21.1. A Data Breach Response Team composed of at least five (5) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effect of the breach.
- 6.21.2. The Data Breach Response Team is composed of the following:
  - 6.21.2.1. Director for Administration - to ensure Management's commitment to breach response, planning and execution;
  - 6.21.2.2. Head Administrator of Marketing and Communications Office - to ensure that an accurate account of any issues is communicated to stakeholders and the press;
  - 6.21.2.3. Data Protection Officer - to ensure that any evidence collected maintains its value in the event that the company chooses to take legal action and also to provide advice regarding liability issues when an incident affects data subjects and/or the general public;
  - 6.21.2.4. Head Administrator of TMC - to work directly with the affected network to research the time, location, and details of a breach;
  - 6.21.2.5. Head Administrator of the Source of Breach - to ensure that there is cooperation in the investigation and securing evidence in his office, department or unit;
  - 6.21.2.6. Head Administrator of Safety and Security - to conduct investigation in cases of physical break-in.
- 6.21.3. LSGH makes every effort to avoid data privacy security incidents, however, it is possible that such incidents will occur on occasions. Data privacy security incidents might occur through:
  - 6.21.3.1. Accidental or unauthorized access to student, employee/personnel or third party personal information;
  - 6.21.3.2. Unauthorized access of personal information from LSGH's server or through malicious attack;
  - 6.21.3.3. Negligence (e.g. leaving a password list in a publicly accessible location);
  - 6.21.3.4. Policy or system's failure;
  - 6.21.3.5. Loss through negligence, theft or robbery of USB, , personal computer, school- issued devices, any removable media containing one or more personal data;
  - 6.21.3.6. Inadvertent exposure of personal data in the LSGH website, social media or public document;
  - 6.21.3.7. Accidental or unauthorized disclosure of personal data (e.g. via misaddressed correspondence or incorrect system permissions/filter failure);
  - 6.21.3.8. Corruption or unauthorized modification of vital records (e.g. alteration of master records);
  - 6.21.3.9. Computer system or equipment compromise (ex. virus, malware, denial of service attack);
  - 6.21.3.10. Compromised IT user account (e.g. spoofing, hacking, shared password);
  - 6.21.3.11. Break in at a location holding personal Information or containing critical information processing equipment such as servers.

**6.22. Notification Protocol**

- 6.22.1. Immediately upon knowledge and discovery of the Security Incident/Personal Data Breach, the employee/personnel, student or parent shall file a Data Breach Reporting Form within 24 hours from knowledge or discovery of personal data breach or he/she should immediately contact the DPO at dpo@lsgh.edu.ph and follow the instructions in the personal data breach procedure as provided in the Data Privacy Incident and Breach Management Policy. All evidence relating to personal data breaches in particular must be retained to enable LSGH to maintain a record of such breaches.
- 6.22.2. Based on the Data Breach Reporting Form, the Data Protection Officer



(DPO) shall assess the reported incident and if verified that a breach has occurred, the DPO shall convene the Data Breach Response Team in case of data breach

- 6.22.3. The DPO shall report a data breach to the National Privacy Commission (NPC) if the personal information believed to have been compromised involves:
  - 6.22.3.1. Information that would likely affect national security, public safety, public order, or public health;
  - 6.22.3.2. At least one hundred (100) individuals;
  - 6.22.3.3. Information required by applicable laws or rules to be confidential; and
  - 6.22.3.4. Personal information of vulnerable groups.
- 6.22.4. The DPO shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report to be submitted to the LSGH President and the National Privacy Commission, within the prescribed period.
- 6.22.5. The DPO and/or Head of the Data Breach Response Team shall inform the President's Council of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law.
- 6.22.6. LSGH shall implement measures to prevent and minimize future occurrence of breaches and security incidents.
- 6.22.7. LSGH shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitoring for security breaches and vulnerability scanning of computer networks.
- 6.22.8. Employee/Personnel directly involved in the processing of personal data must attend training and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in LSGH.

6.23. **Procedure for Recovery and Restoration of Personal Data**

LSGH shall always maintain a back-up file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the back-up with the affected file to determine the presence of any inconsistencies or alteration resulting from the incident or breach.

6.24. **Inquiries and Complaints**

- 6.24.1. Every data subject has the right to reasonable access to his or her personal data being processed by the School.
- 6.24.2. Other Available Rights Include:
  - 6.24.2.1. right to dispute the inaccuracy or error of the personal data;
  - 6.24.2.2. right to request suspension, withdrawal, blocking, removal or destruction of personal data; and
  - 6.24.2.3. right to complain and be indemnified for damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data. Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to the School shall be received and acted upon.
- 6.24.3. Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the School, including data privacy and security policies implemented to ensure the protection of their personal data. They may write to the School at [dpo@lsgh.edu.ph](mailto:dpo@lsgh.edu.ph) and briefly discuss the inquiry, together with details for reference.
- 6.24.4. Complaints shall be filed in three (3) printed copies, or sent to [dpo@lsgh.edu.ph](mailto:dpo@lsgh.edu.ph). The concerned department shall confirm with the complainant its receipt of the complaint.

7. **Sanction**

All employees processing personal data on behalf of LSGH must read these guidelines and failure to comply with these guidelines may result in disciplinary and/or legal action. Disciplinary sanctions shall be in accordance with LSGH's Institutional Office Manual for employees/personnel and LSGH's Student Formation Handbook for students.

## Annexes

### Annex A

#### Data Privacy Notice (Template)

##### Privacy Notice

La Salle Green Hills respects your right to privacy and is committed to protect the confidentiality of your personal information thus has adopted necessary measures to secure it. LSGH is bound to comply with the Data Privacy Act of 2012 (RA 10173), its Implementing Rules and Regulations and relevant issuances of the National Privacy Commission.

##### Information Processed

We collect your personal data that include those you provide us during your application for admission and information we acquire or generate upon enrolment and during the course of your stay with LSGH.

The following personal information are processed:

What information do we collect/process? _____ _____
---

##### Collection

How do we collect the data?

---

---

---

### Use

What is the purpose/use of the collection/processing?  
The information you provide is used for:

---

---

---

We also use the information gathered from you for systems administration purposes and abuse prevention.

Your personal information is accessed and used by:

Who will have access to the data?

---

---

---

Who do we share the data with?

---

---

---

LSGH use and share your information as permitted or required by law to pursue the school's legitimate interests as an educational institution, including a variety of academic, administrative, historical, and statistical purposes.

### Information Protection

LSGH shall store the data collected in the Learning Management System Database.

LSGH shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data which we collected.

LSGH has reasonable organizational, physical and technical security measures in place to help protect against the loss, misuse, and alteration of the information under our control. However, no method of transmission over the Internet or method of electronic storage is 100% secure.

### Retention Period

LSGH shall only retain the said personal information until it serves the purpose. It is collected and processed, after which it shall be securely disposed of.

You may request access to your personal information, and/or have it corrected, erased or blocked on reasonable grounds. LSGH will consider the request and reserves the right to deal with the matter in accordance with law.

### Amendment/Modification of Data Privacy Policies

LSGH reserves the right to modify/amend this notice at any time in its sole discretion. The modification shall take effect immediately upon posting.

Queries and complaints can be directed to the Data Protection Officer via email at [dpo@lsg.edu.ph](mailto:dpo@lsg.edu.ph).

**Annex B**  
**Personal Data Inventory**

Click the link to view the Google Sheet: [Personal Data Inventory](#)

**La Salle Green Hills**

Personal Data Inventory

Office: 

--

Data Subject(s): 

--

Date Prepared: 

--

Provide brief description of the of the Program, Project, Process, Measure, System or Technology for which the PDI was conducted, including the expected benefits (PPPMST): 

--

What information do we collect/process? (Personal Data Collected)	What kind of Personal Data is collected? (Type of Personal Data)	How do we collect the data? How data is collected (Mode?)	Description of Processing		Users			Policy		
			What is the purpose/use of the collection/processing?	What is the Legal Basis	How or where do we store the data? (Data Storage)	Who will have access to the data? Data Access	Data shared (Internal)	Who do we share the data with? - (Data shared -External)	What measures do we have in place to protect the data? (Measures to protect data)	How long will we keep the data? (Data Retention)

**Annex C**  
**LSGH Privacy Impact Assessment**

Click the link to view the Google Sheet: [Privacy Impact Assessment](#)

**Privacy Impact Assessment**

**La Salle Green Hills**

Office: 

--

Data Subject(s): 

--

Date Prepared: 

--

Provide brief description of the of the Program, Project, Process, Measure, System or Technology for which the PDI was conducted, including the expected benefits (PPPMST): 

--

Executive Summary										
Benefit to Organization										
Benefit to Data Subjects										
Privacy Risk to Data Subjects										
Controls – Cost and Complexity										
Overall Impact Assessment										

Privacy Risk Description <small>Provide brief description of the of the Program, Project, Process, Measure, System or Technology for which the PDI was conducted, including the expected benefits.</small>	Type of Privacy Risk	Privacy Risk Causes	Privacy Risk Consequences	Existing Controls	Severity <small>Refer to the Risk Rating Legend</small>	Occurrence <small>Refer to the Risk Rating Legend</small>	Risk Rating <small>(Impact x Occurrence) Refer to the Privacy Risk Rating Legend</small>	Mitigation Actions	Risk Owner	Review Date

**Annex D**

**DATA PRIVACY SECURITY INCIDENT REPORTING FORM**

This document ensures that in the event of a data privacy security incident. All needed information is gathered to understand the impact of the incident and what must be done to reduce any risk to data subject and/or the School's data and information.

The checklist can be accomplished by an individual with knowledge of the incident. It will also require the review by the School's Data Protection Officer who will determine the implications of the Data Privacy Act of 2012, its Implementing Rules and Regulations and/or relevant order and other guidelines issued by the National Privacy Commission and address changes required to the existing processes.

**DATA PRIVACY NOTICE**

LSGH respects one's rights to data privacy. Any personal data that is provided will only be used in line with the investigation of this incident and other legitimate purposes. This includes contact information should there be need for clarifications or additional information. All collected data will be kept secure and confidential, unless otherwise authorized by law. They will be disposed of as soon as it has served its purpose. Aggregated or anonymized data may be retained for statistical or research purposes.

If there are questions or clarifications relating to privacy and data protection, you may contact the College's data protection officer at [dpo@lsg.edu.ph](mailto:dpo@lsg.edu.ph)

Reported by: _____ Name and Signature	Noted by: _____ Name and Signature of Department Head
Department/Unit: _____	Date: _____

**Summary of the Incident**

Date and Time of the Incident	
Date Reported	
How many individuals or records are involved?	
Department/Center/Office	
Nature of the breach: Confidentiality/Integrity/Availability This should be as detailed as possible (e.g. unauthorized access/processing)	
Description of how the breach happened	<brief description of the incident>

**Timeline**

Provide a comprehensive account of the incident.

List down the relevant events in a chronological order, starting from the time the issue was discovered until it was mitigated or resolved, if so.

Date	Time	Particulars

**Personal Data Involved**

Personal Information	Sensitive Personal Information

**Reporting**

Were there any controls in place? (e.g. encryption, etc.)	
--	--

Who detected the breach?	
When was the breach isolated?	

**Initial Assessment**

Does it involve sensitive personal information or any other data that may be used to commit identity fraud?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Uncertain
Is there reason to believe that the data has been acquired by an unauthorized person?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Uncertain
Is there a real risk of serious harm to the affected individual/s?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Uncertain
What are the immediate consequences of the incident on the affected individual/s? (if known)			
Were there security measures in place to help avoid the incident or mitigate its negative impact? If yes, please describe.			

**Remedial Measures Taken**

Measure	Application	Date (of implementation)
What have you done to secure, recover, remove, or delete the personal data (if applicable)?		
What have you done to help mitigate the harm, damage, distress or negative consequences caused by the incident on the affected individuals?		
What have you done to inform the affected individuals? Indicate the reason if there was delay, or no notification.		
What have you done to provide assistance to affected individuals?		
What have you done to prevent or avoid similar incidents in the future?		

**Impact**

What are the potential adverse consequences for students, personnels, third parties, or LSGH?	
What processes/systems are affected and how? (e.g. website taken off line, access to data base restricted, etc.)	
Have you received a formal complaint from any individual affected by this incident/breach? If so, provide details.	

**Management**

What further action has been taken to minimize the possibility of a repeat of such an incident?	
---	--

**Assessment (to be accomplished by Data Protection Officer)**

Recommendation:
-----------------

**REFERENCES**

LAWS:

Republic Act 10173, Data Privacy Act of 2012

Implementing Rules and Regulations of the Data Privacy Act of 2012

NPC Circular 16-03 – Personal Data Breach Management

URL GENERAL WEBSITE ARTICLE WITHOUT AUTHOR)

<https://www.ed.ac.uk/records-management/policy/data-protection>

<https://www.nottingham.ac.uk/governance/records-and-information-management/data-protection/data-protection-policy.aspx>

<https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design>