	LA SALLE GREEN HILLS			
	DOCUMENT TITLE: Data Privacy Policy		**DOCUMENT NO:**	**CLASS:**
	FILES SOURCE:	**EFFECTIVE DATE:**	**APPROVAL DATE:**	**NO. OF PAGES: 20**

APPROVAL HISTORY

Date (YYYY-MM-DD)	Prepared by:	Authorized by:	Approved by: (Secondary)	Approved by:
	Atty. Armee M. Javellana			

REVISION HISTORY

Revision Date (YYYY-MM-DD)	Author	Reason for Changes
		Initial Documentation

RELATED INFORMATION

Document Control No.	Document Title	File Source

TABLE OF CONTENTS

CONTROL STAMP

FOR CIAD USE ONLY

1. Introduction

La Salle Green Hills (LSGH) collects, uses, stores and processes personal information relating to potential, current and former employees and students, alumni, website users and other relevant third parties, referred to this in this policy as data subjects. As Data Privacy has become 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 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. Objectives

2.1 To ensure clarity and consistency about how personal data must be processed and the LSGH expectations for all those who process personal data on its behalf
2.2 To ensure compliance with the Data Privacy Act and other relevant legislations and regulations
2.3 To protect LSGH's reputation by ensuring the personal data entrusted to it is processed in accordance with data subject rights
2.4 To protect LSGH from risks of personal data incidents or breaches and other breaches of data protection law
2.5 To embed a culture of privacy that enables compliance
2.6 To establish effective privacy practices, procedures and systems
2.7 To evaluate LSGH's privacy practices, procedures and systems to ensure continued effectiveness
2.8 To enhance response to privacy issues
2.9 To promote a culture of trust and respect that enables community building

3. Definition of Terms

3.1 Data Subject -refers to an individual whose personal data is processed by LSGH;
3.2 Student – an individual officially enrolled in LSGH
3.3 Former Student – an individual who enrolled but is no longer enrolled in LSGH
3.4 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

3.5 Former employees – employees who are retired, resigned, terminated or contract has ended

3.6 Alumni – an individual who studied in LSGH for at least two (2) years

3.7 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.

3.8 Processor – individual/department/unit which processes personal data in behalf of LSGH

3.9 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

3.10 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

3.11 Personal Data – used when personal information, sensitive personal information and privileged information are referred to collectively

3.12 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.

3.13 Sensitive Personal Information – refers to personal information:

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

3.13.2 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;

3.13.3 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;

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

3.14 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.

3.15 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.

3.16 Privacy as a default setting – systems, processes or practices in LSGH is designed to protect personal data automatically.

3.17 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.

3.18 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

3.19 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

3.20 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 Team.

3.21 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

3.22 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

3.23 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

3.24 Direct Marketing – refers to communication be 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. Scope

This policy applies to all departments and units of LSGH, employees (regardless of classification), students and third party contractors/processors who processes personal information collected by LSGH or in 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 process regardless of the location where that personal data is stored (e.g. on employee's own device) and regardless of the data subject.

5. Guideline Statements

5.1 All employees, students and third party contractors/processors processing personal data in behalf of LSGH must read the policy and failure to comply to this policy may result to disciplinary and/or legal action. Disciplinary sanctions shall be in accordance to LSGH's Institutional Office Manual or Student Handbook.

5.2 Personal Information includes but are not limited to the following:

- Name
- Date and place of birth
- Name of parents/guardian/children/siblings
- Address
- Email Address
- Telephone/Mobile Number
- Field of Study
- Dates of attendance
- Grade Level and Section
- Grades
- Previous Educational Institution Attended
- Date of Graduation
- Degrees/Awards/Honors/Scholarships/Grants received
- Height and weight information
- Performance records and participation in competitive events and officially recognized activities, sports, and organizations

- Photographs/Videos/Images of individual or in groups
- Recordings from closed-circuit television

5.3 Sensitive Personal Information include but are not limited to the following:

- Ethnicity
- Gender/Sexual orientation/Gender Identity
- Religion
- Disability/Special Education Needs Conditions
- Disciplinary records
- Guidance records
- Health records
- Financial records
- Alien Certificate/Visa/ Passport information
- Performance evaluation
- Government issued identification numbers (TIN, SSS, PhilHealth, Pag-Ibig, etc.)
- Student/Employees LSGH identification numbers
- Licenses

5.4 Personal data collected shall be processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

5.4.1 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 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.

5.4.1.1 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.

5.4.2 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.

5.4.2.1 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.

5.4.3 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 processes should not be collected.

5.4.4 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.

5.5 Lawful processing of personal information can be any of the following:

5.5.1 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

5.5.2 The processing is required due to a contract

5.5.3 It is necessary due to a legal obligation

5.5.4 The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;

5.5.5 The processing is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law

5.5.6 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.

5.6 Lawful processing of sensitive personal information or privileged information can be any of the following:

5.6.1 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

5.6.2 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

5.6.3 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;

5.6.4 The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations provided that:

5.6.4.1 Processing is confined and related to the bona fide members of these organizations or their associations;

5.6.4.2 The information is not transferred to third parties; and

5.6.4.3 Consent of the data subject was obtained prior to processing;

5.6.5 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

5.6.6 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.

5.7 Security measures for protection of personal information

5.7.1 Organizational Measures

5.7.1.1 LSGH shall appoint a Data Protection Officer and such appointment shall be registered with the National Privacy Commission

5.7.1.2 LSGH shall adopt the Privacy by Design (PbD) Framework in processing personal data.

5.7.1.3 LSGH shall develop a Privacy Management Plan.

5.7.1.4 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).

5.7.1.5 Every office, department and unit must nominate one or more Compliance Officer for Privacy (COP), who will act as the data protection champion of the department or unit. These individuals are the first point of contact for data protection questions in their area. They shall escalate difficult questions to the Data Protection Officer (DPO) and act as a channel of communication between the DPO and their office.

5.7.1.6 All heads of departments are responsible for ensuring that all associates 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 schools and departments.

5.7.1.7 LSGH shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.

5.7.1.8 All employees will be asked to sign a Confidentiality and Non-Disclosure Agreement.

5.7.1.9 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.

5.7.1.10 Data privacy protection shall be part of employee's term and conditions of employment, breach of data privacy policy due to unauthorized access misuse or loss may result to 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.

5.7.1.11 LSGH through the Risk Management Compliance Office shall provide capacity building, orientation or training programs associates regarding privacy or security policies. There shall be a 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 trainings and orientations regularly.

5.7.1.12 The Risk Management Compliance Office will do periodic audits to ensure compliance with this policy and the DPA.

5.7.1.13 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.

5.7.2 Physical Measures

5.7.2.1 Each office, department or unit involved in processing of personal information shall:

5.7.2.1.1 Create and implement guidelines to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;

5.7.2.1.2 Design of office space and work stations, including the physical arrangement of furniture and equipment, which provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

5.7.2.1.3 Clearly define duties, responsibilities and schedule of individuals involved in the processing of personal data thus limiting access on a need to know basis.

5.7.2.1.4 Create and implement guidelines regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data;

5.7.2.1.5 Prevent the mechanical destruction of files and equipment containing and/processing personal information. The area used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

5.7.3 Technical Measures

5.7.3.1 Where appropriate LSGH shall adopt the following measures:

5.7.3.1.1 Info Security, IT Security and Infonet Policy with respect to the processing of personal data

5.7.3.1.2 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;

5.7.3.1.3 The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

5.7.3.1.4 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

5.7.3.1.5 The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

5.7.3.1.6 A process for regularly penetration testing, assessing, and evaluating the effectiveness of security measures;

5.7.3.1.7 Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

5.8 Privacy Notices

5.8.1 LSGH and all department and units processing personal data must provide data subject 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 group 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.

5.9 Data Retention and Disposal

5.9.1 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.

5.9.2 If the data is no longer required, it must be securely disposed by shredding or by deletion.

5.9.3 The office, department or unit must set its own retention schedules based on legal and business requirements or based on industry practice.

5.10 Privacy by Design Framework (PbD). By applying PbD framework LSGH shall:

5.10.1 Take a proactive rather than a reactive measure. It anticipates the risks and prevents privacy incidents before they occur.

5.10.2 Seek to deliver the maximum degree of privacy by ensuring personal information are automatically protected as a practice. No action on the part of the individual is needed in order to protect their privacy.

5.10.3 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.

5.10.4 Seek to accommodate all legitimate objectives in a positive-sum "win-win" manner

5.10.5 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.

5.10.6 Seek to assure all stakeholders that whatever the business practice and technology involved is operating in accordance to the objectives of this policy

5.10.7 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.

5.10.8 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.

5.10.9 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.

5.11 Personal Data Inventory (Annex B)

5.11.1 Each department or unit shall accomplish a 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:

5.11.1.1 Personal data collected and processed

5.11.1.2 Purpose of the collection/processing of the personal data

5.11.1.3 Owner of the personal data

5.11.1.4 Legal basis of the collection/processing

5.11.1.5 Storage location of data including third party systems and where their servers are located

5.11.1.6 Mapping where the data goes from point of collection internally and externally

5.11.1.7 Access control to data (read only or can edit)

5.11.1.8 Existing policies if there are any on use, disclosure, protection, back-up and disposal policies

5.11.1.9 Period of retention of data and format of data

5.12 Privacy Impact Assessment

5.12.1 When considering new processing activities or setting up new procedures or systems that involve personal information, the office, department or unit must always be 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 putting 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".

5.12.2 A PIA should be conducted in the following cases:

5.12.2.1 the use of new technologies or changing technologies (programs, systems or processes);

5.12.2.2 automated processing including profiling;

5.12.2.3 large scale processing of sensitive data;

5.12.2.4 large scale and systematic monitoring of publicly accessible areas (e.g. CCTV)

5.12.3 A PIA must include:

5.12.3.1 Description of the program, project, process, measure, system or technology and including expected benefits which requires the collection of personal information

5.12.3.2 Description of the information lifecycle including personal information data process flow

5.12.3.3 Description of legal grounds for processing personal information including copies of forms used (e.g. consent forms)

5.12.3.4 Identification of the privacy risks and type of risks

5.12.4 Risk Map

5.12.4.1 A Risk Map is an assessment of the severity and likelihood of identified risks

5.12.4.2 It includes a list of proposed controls with type (organizational, physical, or technical), estimated cost, and estimated implementation timeframe

5.13 Hiring Third Party Processors or Personal Information Processors (PIP)

5.13.1 Where external processors are hired to process personal information on behalf of LSGH:

5.13.1.1 Personal Information Processor (PIP) must be chosen by LSGH which provide sufficient guarantees about security measures to protect the processing of personal data

5.13.1.2 LSGH must take reasonable steps that security measures are in place

5.13.1.3 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.

5.14 Personal Information/Data for Research

5.14.1 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: informed and freely given consent, public interest, legitimate or contract

5.14.2 Research subject's/participants' data privacy shall be protected. Thi includes but are not limited to the following:

5.14.2.1 The research subjects must be aware how their data will be used and may object if they wish

5.14.2.2 Personal data should be kept confidential and can only be shared with research subject's permission

5.14.2.3 There should be no substantial damage or distress to research subjects

5.14.2.4 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.

5.14.2.5 There should be anonymizing or pseudonymizing of data whenever possible

5.14.2.6 Ensure the personal information is kept secured and only accessed by those authorized to do so

5.15 Data Subject Rights

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

5.15.1.1 Right to be informed

5.15.1.1.1 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.

5.15.1.1.2 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:

5.15.1.1.2.1 Description of the personal data to be entered into the system

5.15.1.1.2.2 Purposes for which information are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose

5.15.1.1.2.3 Basis of processing, when processing is not based on the consent of the data subject

5.15.1.1.2.4 Scope and method of the personal information processing

5.15.1.1.2.5 The recipients of the personal information or to whom it may be disclosed

5.15.1.1.2.6 Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized

5.15.1.1.2.7 The identity and contact details of the personal information controller or its Data Protection Officer (DPO)

5.15.1.1.2.8 The period for which the information will be stored

5.15.1.1.2.8.1 The existence of their rights as data subjects

5.15.1.2 Right to object

5.15.1.2.1 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.

5.15.1.2.2 When a data subject objects or withholds consent, the processor shall no longer process the personal data, unless:

5.15.1.2.2.1 The personal data is needed pursuant to a subpoena;

5.15.1.2.2.2 The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service 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

5.15.1.2.2.3 The information is being collected and processed as a result of a legal obligation.

5.15.1.3 Right to Access.

5.15.1.3.1 The data subject has the right to reasonable access to, upon demand, the following:

5.15.1.3.1.1 Contents of personal information of the data subject that were processed

5.15.1.3.1.2 Sources from which personal data were obtained

5.15.1.3.1.3 Names and addresses of recipients of the personal information

5.15.1.3.1.4 Manner by which such data were processed

5.15.1.3.1.5 Reasons for the disclosure of the personal information to recipients, if any

5.15.1.3.1.6 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

5.15.1.3.1.7 Date when his or her personal data concerning the data subject were last accessed and modified

5.15.1.3.1.8 The designation, name or identity, and address of the personal information controller.

5.15.1.4 Right to rectification/correction

5.15.1.4.1 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.

5.15.1.4.2 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.

5.15.1.5 Right to Erasure or Blocking

5.15.1.5.1 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:

5.15.1.5.2 The personal information is incomplete, outdated, false, or unlawfully obtained

5.15.1.5.3 The personal information is being used for purpose not authorized by the data subject

5.15.1.5.4 The personal information is no longer necessary for the purposes for which they were collected

5.15.1.5.5 The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing

5.15.1.5.6 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

5.15.1.5.7 The processing is unlawful

5.15.1.5.8 The processor violated the rights of the data subject

5.15.1.5.9 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 subject may object to further processing of their personal information.

5.15.1.5.10 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

5.15.1.6 Right to Data Portability

5.15.1.6.1 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.

5.15.1.7 Right to damages.

5.15.1.7.1 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.

5.15.1.8 Right to file a complaint

5.15.1.8.1 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 subject access request has been received.

5.15.1.8.2 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.

5.16 Where the legal basis of processing is consent, data subject may withdraw consent. When withdrawing consent, the data subject need to demonstrate valid and reasonable grounds for withdrawal relating to their particular situation.

5.17 Data subject 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 demonstrate 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.

5.18 Rights in Relation to Automated Decision Making and Profiling

5.18.1 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.

5.19 Record Keeping

5.19.1 LSGH shall keep full and accurate records of all its data processing activities. Office, 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.

5.19.2 These records should include, at a minimum, the name and contact details of LSGH as Personal Information Controller (PIC) and 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

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

5.19.3.1 Facts surrounding the breach

5.19.3.2 Effects of the data breach; and

5.19.3.3 Remedial action taken

5.20 Access

5.20.1 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.

5.20.2 A school official is:

5.20.2.1 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.

5.20.2.2 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

5.20.2.3 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.

5.20.2.4 An individual serving on the Board of Trustees.

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

5.20.3.1 Performing a task that is specified in his/her position description or contract agreement.

5.20.3.2 Performing a task related to the discipline of a student/employee.

5.20.3.3 Providing a service or benefit relating to the student or student's family or employee or employee's family, such as health care, counseling, job placement, or financial aid discipline cases

5.20.3.4 Maintaining the safety and security of the campus.

5.21 Data Sharing

5.21.1 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.

5.21.2 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.

5.21.3 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.

5.21.4 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.

5.21.5 If transferring personal information outside the Philippines, associates involved in transferring personal information must inform first the DPO to ensure that appropriate safeguards are in place before agreeing to any such transfer. Personal information can be transferred in the following cases:

5.21.5.1 Data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

5.21.5.2 The transfer is necessary for one of the other reasons set out in the EU General Data Protection Regulation (GDPR) including:

5.21.5.3 The performance of a contract between LSGH and the data subject (e.g. student exchange program).

5.21.5.4 Reasons of public interest

5.21.5.5 To establish, exercise or defend legal claims or

5.21.5.6 To protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.

5.21.6 LSGH has a full range of standard transfer agreements and clauses and you should seek guidance from the DPO at dpo@lsgh.edu.ph before any transfer of personal data takes place.

5.22 Disclosure

5.22.1 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.

5.22.2 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 the student's records.

5.22.3 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 you need guidance, please contact the DPO.

5.22.4 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. For guidance, please contact the DPO.

5.23 Direct Marketing

5.23.1 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.

5.24 Responsibilities of the Data Protection Officer

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

5.24.2 The DPO is responsible for:

5.24.2.1 Advise LSGH and the community (associates and students) of its obligation under the DPA

5.24.2.2 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.

5.24.2.3 Provide advice where requested on data privacy concerns

5.24.2.4 Cooperate with and act as the point of contact for the NPC

5.25 Responsibilities of LSGH

5.25.1 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.

5.26 Responsibilities of Personnel and Student Processing Personal Information

5.26.1 Personnel and student processing personal information shall ensure that:

5.26.1.1 All personal information is kept securely
5.26.1.2 No personal information is disclosed either verbally, writing or electronically, accidentally or otherwise, to any unauthorized third party
5.26.1.3 Personal information is kept in accordance with the LSGH's retention schedule
5.26.1.4 Any queries regarding data protection, including data subject access requests and complaints, are promptly directed to the Data Protection Officer
5.26.1.5 Any data protection incidents are swiftly brought to the attention of the Data Protection Officer and support in resolving breaches
5.26.1.6 Where there is doubt or uncertainty around a data protection concern, advice should be sought from the Data Protection Officer.
5.26.1.7 Where associates are responsible for supervising students doin 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.

5.26.2 Associates 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.

5.27 Contractors, Short Term or Voluntary Staff (including on the job trainees, interns)

5.27.1 Heads of office, departments or units who employ contractors, short term or voluntary staff shall:

5.27.1.1 Ensure contractors, short term or voluntary staff sign a Confidentialit and Non-Disclosure Agreement
5.27.1.2 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.
5.27.1.3 Appropriately appraise Contractors, Short Term or Voluntary Staff for the data they will be processing

5.27.1.4 Ensure that Contractors, Short Term or Voluntary Staff comply with the following:

5.27.1.5 Keep secure and confidential any personal data collected or processed in the course of work undertaken for LSGH

5.27.1.6 Return to LSGH all personal data upon completion of the work, including any copies that may have been made.

5.27.1.7 Notify LSGH of any disclosure of personal information to any other organization or any person who is not a direct employee of the contractor

5.27.1.8 Not to store nor process any personal data made available by LSGH, or collected in the course of work outside the Philippines, unless there is a written consent to do so has been received by LSGH.

5.28 Employees and Students are responsible for:

5.28.1 Familiarizing themselves with the privacy notice provided when they register with LSGH:

5.28.2 Ensuring that the personal information they provided to LSGH are accurate and up to date.

5.29 Breach and Security Incidents

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

5.29.2 Creation of Data Breach Response Team

5.29.2.1 A Data Breach Response Team comprising 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.

5.29.2.2 The Data Breach Response Team is composed of the following:

- Director of Administration - to ensure management's commitment to breach response planning and execution
- Head Administrator of Marketing Communication Office - to ensure an accurate account of any issues is communicated to stakeholders and the press
- 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
- Head Administrator of TMC - to work directly with the affected network to research the time, location, and details of a breach
- 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.
- Head Administrator of Safety and Security - to conduct investigation in cases of physical break-in.

5.29.3 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:

5.29.3.1 Accidental or unauthorized access to student, employee or third party personal information

5.29.3.2 Unauthorized access of personal information from LSGH's server or through malicious attack

5.29.3.3 Associate negligence (e.g. leaving a password list in a publicly accessible location

5.29.3.4 Policy or system's failure

5.29.3.5 Loss through negligence, theft or robbery of or theft of USB, laptop, personal computer, smart phone, any removable media containing one or more personal data

5.29.3.6 Inadvertent exposure of personal data in the LSGH website, social media or public document

5.29.3.7 Accidental or unauthorized disclosure of personal data (e.g. via misaddressed correspondence or incorrect system permissions/filter failure)

5.29.3.8 Corruption or unauthorized modification of vital records (e.g. alteration of master records)

5.29.3.9 Computer system or equipment compromise (ex. virus, malware, denial of service attack)

5.29.3.10 Compromised IT user account (e.g. spoofing, hacking, shared password)

5.29.3.11 Break in at a location holding personal Information or containing critical information processing equipment such as servers

5.29.4 Notification Protocol

5.29.4.1 Immediately upon knowledge and discovery of the Security Incident/Personal Data Breach, the personnel or student 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.

5.29.4.2 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

5.29.4.3 The DPO shall report a data breach to the National Privacy Commission (NPC) if the personal information believed to have been compromised involves:

5.29.4.3.1 Information that would likely affect national security, public safety, public order, or public health

5.29.4.3.2 At least one hundred (100) individuals

5.29.4.3.3 Information required by applicable laws or rules to be confidential

5.29.4.3.4 Personal information of vulnerable groups

5.30 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.

5.31 The DPO and/or Head of the Data Breach Response Team shall inform th 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.

5.31.1 LSGH shall implement measures to prevent and minimize future occurrence of breaches and security incidents.

5.31.1.1 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. 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.

5.31.1.2 Procedure for recovery and restoration of personal data

5.31.1.2.1 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. Inquiries and Complaints

6.1 LSGH must have a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to LSGH shall be received and acted upon.

6.2 Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of LSGH, including data privacy and security policies implemented to ensure the protection of their personal data. They may write to dpo@lsgh.edu.ph and briefly discuss the inquiry, together with details for reference.

6.3 Complaints shall be filed in three (3) printed copies with the Data Protection Office, or sent to dpo@lsgh.edu.ph.

6.4 Review of Policy

6.4.1 This policy shall be reviewed every three (3) years to ensure that it is updated and relevant to the needs of LSGH and the community.

6.5 LSGH Contacts

The LSGH's named Data Protection Officer is Atty. Armee M. Javellana.

Inquiries regarding this policy must be addressed to dpo@lsgh.edu.ph

Annex A

Click the link to view the Google Form: Data Privacy Security Incident Reporting Google Form

Data Privacy Security Incident Reporting Form

This document ensures that in the event of a security incident such as data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk to the data subject and/or the LSGH'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 LSGH'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.

Name of individual reporting:_____
Office, Department or Unit (If Student - Grade and Section): **_____**
Date: _____
Summary of the Incident

Data and Time of the Incident _____
How many individuals or records are involved?_____
Office, Department or Unit (If Student - Grade and Section) _____
Nature of the Breach: Confidentiality/Integrity/Availability (Brief description of the incident or breach, e.g. unauthorized access/processing, loss of gadget, loss of laptop) _____ _____ _____
Description of how the breach happened _____ _____ _____
What type of data is involved? (The individual data fields should be identified, e.g. name, address, bank account number, etc.) _____ _____ _____
What happened to the data? _____ _____ _____

Reporting
When was the breach reported? _____ _____
Were there any controls in place? (e.g. encryption, etc.) _____ _____
Who detected the breach? _____ _____ _____
When was the breach isolated? _____ _____

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

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

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