



Policy and Procedure

Name: Personal Data Protection

Approved by: Board of Directors

Last reviewed: 11 April 2017

SWINBURNE
UNIVERSITY OF
TECHNOLOGY
SARAWAK CAMPUS

SECTION 1 - INTRODUCTION	2
PURPOSE	2
SCOPE	2
DEFINITIONS	2
LEGISLATIVE CONTEXT	4
SECTION 2 - POLICY	5
PRINCIPLES	5
POLICY	6
SECTION 3 - PROCEDURE	11
PROCEDURE	11
SUPPORTING DOCUMENTATION	19
SECTION 4 - GOVERNANCE	20
RESPONSIBILITY	20
VERSION CONTROL AND CHANGE HISTORY	20
POLICIES & REGULATIONS DIRECTORY REQUIREMENTS	21

SECTION 1 - INTRODUCTION

PURPOSE

This is to establish a policy and procedure that must be observed in relation to the collection, use, storage, security and disclosure of personal information, including sensitive personal information by, or for Swinburne University of Technology Sarawak Campus so that the university complies with the [Personal Data Protection Act 2010](#) ('PDPA' or 'the Act'), enforced on 15 November 2013.

SCOPE

This policy and procedure applies to all staff and students of Swinburne University of Technology Sarawak Campus ("Swinburne Sarawak") as well as third parties, in a commercial transaction with Swinburne Sarawak.

DEFINITIONS

Word/Term	Definition
Advisory Guidelines	Guidelines issued by the Malaysian Personal Data Protection Department (<i>Jabatan Perlindungan Data Peribadi Malaysia</i>) to provide guidance on the manner in which the Department will interpret provisions of the PDPA. The Guidelines serve as recommended best practices to help individuals and organisations comply with the PDPA. Where relevant, reference is made to the provisions of the PDPA.
CCTV*	A closed circuit television/ surveillance system that uses video cameras and related equipment for security purposes.
Commercial Transactions**	Any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.
Commissioner**	The Personal Data Protection Commissioner appointed under Section 47 of the PDPA.
Data Processor**	Any person, other than a staff member of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his/ her own purposes.
Data Subject**	An individual who is the subject of the personal data, such as Swinburne Sarawak students, staff and third parties.
Data User**	A person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor.
Direct Marketing***	The communication by whatever means of any advertising or marketing material which is directed to particular individuals.
Disclose/ Disclosure**	An act by which such personal data is made available by a data user.
Head of Management Unit	The position with management responsibility for a management unit.
M&C	Marketing & Communications
Management Unit	A unit/ faculty (this excludes sub-units or sub-sections or specific portfolios within a unit/ faculty).
Minister**	The Minister for the Malaysian Ministry of Communication and Multimedia, charged with the responsibility for the protection of personal data.
Personal Data**	Any information in respect of commercial transactions, which: a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

Word/Term	Definition
	<p>b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or</p> <p>c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010. For example, name, address, date of birth, telephone number, photographs, videos, etc.</p>
Personal Data Register	A document which keeps track of the personal data processed by the University, including details such as the categories of personal data collected, the purpose of processing the personal data, the first point of collection and retention period.
Processing**	<p>Collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including:</p> <p>a) the organisation, adaptation or alteration of personal data;</p> <p>b) the retrieval, consultation or use of personal data;</p> <p>c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or</p> <p>d) the alignment, combination, correction, erasure or destruction of personal data.</p>
Relevant Person**	A person who has parental responsibility for the data subject; or a person authorised in writing by the data subject to act on behalf of the data subject; or a person authorised in writing by the data subject to make a data access request or/and data correction request on behalf of the data subject.
Requestor**	The data subject or the relevant person on behalf of the data subject, who has made the request in relation to a data access request or data correction request.
Sensitive Personal Data**	Any personal data consisting of information as to the physical or mental health or condition of a data subject, his/her political opinions, his/her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him/her of any offence or any other personal data as the Minister may determine by order published in the Malaysian Federal Government Gazette.
Third Party**	<p>In relation to personal data, means any person other than:</p> <p>a) a data subject;</p> <p>b) a relevant person in relation to a data subject;</p> <p>c) a data user;</p> <p>d) a data processor; or</p> <p>e) a person authorised in writing by the data user to process the personal data under the direct control of the data user, including all third party suppliers who have entered into any commercial transaction with Swinburne Sarawak.</p>
Written	For the purpose of this document, 'written' may either be physical (i.e. letter) or electronic (i.e. e-mail).

*Source: Introduction section, [Proposal Paper \[No.5/2014\]](#)

**Source: Section 4 Interpretation, [PDPA](#)

***Source: Section 43(5), [PDPA](#)

LEGISLATIVE CONTEXT

Name	Location
Personal Data Protection Act 2010	http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf <i>The Act that regulates the processing of personal data in commercial transactions in Malaysia and to provide on matters connected therewith and incidental thereto.</i>
Personal Data Protection Regulations 2013 P.U.(A) 335/2013	http://www.federalgazette.agc.gov.my/output/pua_20131114_P.U.%20(A)%20335%20-%20PERSONAL_DATA_PROTECTION_REGULATIONS_2013.pdf <i>This document provides further clarifications on the seven (7) principles of the PDPA.</i>
Personal Data Protection (Class of Data Users) Regulations 2013 P.U.(A) 336/2013	http://www.federalgazette.agc.gov.my/output/pua_20131114_P.U.%20(A)%20336-PERINTAH%20PERLINDUNGAN%20DATA%20PERIBADI%20(GOLONGAN%20PENGUNA%20DATA)%202013.pdf <i>This document provides further clarifications on the various classes of data users who must register under the PDPA.</i>
Personal Data Protection (Registration of Data User) Regulations 2013 P.U.(A) 337/2013	http://www.federalgazette.agc.gov.my/output/pua_20131114_P.U.%20(A)%20337%20-%20peraturan-peraturan%20perlindungan%20data%20peribadi%20(pendaftaran%20pengguna%20data)%202013.pdf <i>This document provides further clarifications on the Registration of Data User under the PDPA.</i>
Personal Data Protection (Fees) Regulations 2013 P.U.(A) 338/2013	http://www.federalgazette.agc.gov.my/output/pua_20131114_P.U.%20(A)%20338-PERATURAN-PERATURAN%20PERLINDUNGAN%20DATA%20PERIBADI%20(FI)%202013.pdf <i>This document provides further clarifications on the fees payable for data access request under PDPA and the fees payable to the Commissioner for several cases.</i>
Personal Data Protection Standard 2015	http://www.pdp.gov.my/index.php/en/akta-709/standard <i>This document provides further clarifications on the Security, Retention and Data Integrity Standards.</i>

SECTION 2 - POLICY

PRINCIPLES

Section 2 of the PDPA states that the Act applies to:

- (a) any person who processes; and
- (b) any person who has control over or authorises the processing of, any personal data in respect of commercial transactions,
 - (i) if the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or
 - (ii) if the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.

Section 3 of the PDPA further states that the Act **shall** not apply to:

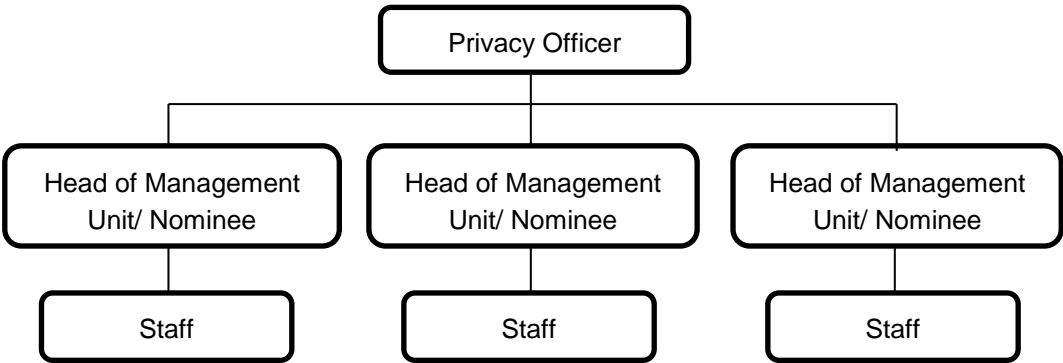
- (a) the Federal Government and State Governments, or
- (b) any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.

This Personal Data Protection Policy and Procedure sets out the responsibilities of all staff and students of Swinburne Sarawak as well as third parties, in a commercial transaction with Swinburne Sarawak, in relation to personal data and sensitive personal data. The aim is to ensure all personal or sensitive personal data processed by Swinburne Sarawak complies with the following Personal Data Protection Principles set forth in the PDPA:

- (a) General Principle;
- (b) Notice and Choice Principle;
- (c) Disclosure Principle;
- (d) Security Principle;
- (e) Retention Principle;
- (f) Data Integrity Principle; and
- (g) Access Principle.

In this policy and procedure, the word **'shall'** or **'must'** is used when it is mandatory to implement the requirement. The word **'should'** is used in statements of best practice, which are strongly recommended for implementation but are not mandatory.

The following Personal Data Protection Governance Structure of Swinburne Sarawak facilitates university-wide implementation of this policy and procedure.



POLICY

1.	Personal Data Protection Principles
1.1	General Principle (Section 6, PDPA)
1.1.1	<p>Swinburne Sarawak shall obtain the data subject’s consent before the processing of any personal data unless it is necessary:</p> <ul style="list-style-type: none"> (a) for the performance of a contract to which the data subject is a party (including but not limited to contract for the provision of services and for employment purposes); (b) for the taking of steps upon the request of the data subject with a view to entering into a contract, including but not limited to employment contracts; (c) for compliance with any legal obligation to which Swinburne Sarawak is the subject, other than an obligation imposed by a contract; (d) in order to protect the vital interests of the data subject; (e) for the administration of justice; and (f) for the exercise of any functions conferred on any person or by or under any law.
1.1.2	<p>Swinburne Sarawak shall only process personal data whereby:</p> <ul style="list-style-type: none"> (a) the personal data is processed for a lawful purpose directly related to the operational functions of Swinburne Sarawak; (b) the processing of the personal data is necessary for or directly related to that purpose; and (c) the personal data is adequate but not excessive in relation to that purpose.
1.1.3	<p>Subject to the conditions in Section 1.1.2 being met, Swinburne Sarawak shall only process sensitive personal data about a data subject in the following situations:</p> <ul style="list-style-type: none"> (a) Explicit consent has been received. (b) The processing is necessary: <ul style="list-style-type: none"> (i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on Swinburne Sarawak in connection with employment; (ii) in order to protect the vital interests of the data subject or another person, in a case where: <ul style="list-style-type: none"> • consent cannot be given by or on behalf of the data subject; or • Swinburne Sarawak cannot reasonably be expected to obtain the consent of the data subject. (iii) in order to protect the vital interests of another person, in a case where consent by, or on behalf of the data subject has been unreasonably withheld; (iv) for medical purposes and is undertaken by: <ul style="list-style-type: none"> • a healthcare professional; • a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional; (v) for the purpose of, or in connection with, any legal proceedings; (vi) for the purpose of obtaining legal advice; (vii) for the purposes of establishing, exercising or defending legal rights; (viii) for the administration of justice;

	<ul style="list-style-type: none"> (ix) for the exercise of any functions conferred on any person by or under any written law; or (x) any other purposes as the Minister charged with the responsibility for the protection of personal data thinks fit. <p>(c) The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.</p>
1.2	Notice and Choice Principle (<i>Section 7, PDPA</i>)
1.2.1	<p>Swinburne Sarawak shall publish a written Privacy Collection Notice that includes the following:</p> <ul style="list-style-type: none"> (a) A statement informing the data subject that his/ her personal data is being processed by or on behalf of Swinburne Sarawak; (b) A clear description of the personal data being collected and/ or processed; (c) A clear description of the purpose(s) for which the personal data is being processed/ and collected; (d) The source of the personal data; (e) A statement informing the data subject on his/ her rights to request access to and to request correction of the personal data; (f) The method of contacting Swinburne Sarawak for any inquiries or complaints in relation to the personal data; (g) The class of third parties to whom Swinburne Sarawak discloses or may disclose the personal data; (h) The choices and means Swinburne Sarawak offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data; (i) Whether it is voluntary or obligatory for the data subject to provide the required personal data; and (j) Where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he/ she fails to supply the personal data.
1.2.2	<p>The Privacy Collection Notice shall be given to the data subject as soon as practicable:</p> <ul style="list-style-type: none"> (a) When Swinburne Sarawak first asks the data subject to provide his/ her personal data; (b) When Swinburne Sarawak first collects the data subject's personal data; or (c) In any other case, before Swinburne Sarawak uses the personal data for a purpose other than the purpose for which the personal data was collected or discloses the personal data to a third party.
1.2.3	Swinburne Sarawak's Privacy Collection Notice shall be made available in the national and English languages.
1.2.4	The data subject shall be provided with a clear and readily accessible means to exercise his/ her choice, where necessary.
1.3	Disclosure Principle (<i>Section 8, PDPA</i>)
1.3.1	Swinburne Sarawak shall notify the data subject before disclosing personal data to a third party by specifying a list of third parties to whom Swinburne Sarawak may disclose the personal data in the Privacy Collection Notice.
1.3.2	Swinburne Sarawak shall obtain consent from the data subject and inform the Privacy Officer:

	<ul style="list-style-type: none"> (a) before disclosing personal data for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purposes related to that purpose that are not listed in the Privacy Collection Notice; or (b) before disclosing personal data to third parties that are not listed in the Privacy Collection Notice.
1.3.3	<p>Personal data shall only be disclosed to a third party, whereby:</p> <ul style="list-style-type: none"> (a) data subjects have been provided with a notification on the disclosure of their personal data; or (b) it is necessary for legal purposes such as to prevent or detect a crime or to comply with requirements by the order of a court; or (c) there are reasonable grounds that disclosure is required to prevent or lessen serious imminent threat to life or health; or (d) the Minister determined that the disclosure was justified as being in the public interest; or (e) Swinburne Sarawak complies with all provisions under Section 1.1: General Principle in this policy and procedure.
1.3.4	<p>The following are exemptions from the PDPA provisions, as stated in Section 45 of the Act:</p> <ul style="list-style-type: none"> (a) Personal data processed for the prevention or detection of crime or for the purpose of investigations; (b) Personal data processed for the apprehension or prosecution of offenders; or (c) Personal data processed for the assessment or collection of any tax or duty or any other imposition of a similar nature; (d) Personal data processed in relation to information of the physical or mental health of a data subject shall be exempted from the Access Principle and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual; (e) Personal data processed for preparing statistics or carrying out research; (f) Personal data that is necessary for the purpose of or in connection with any order or judgement of a court; (g) Personal data processed for the purpose of discharging regulatory functions; (h) Personal data processed only for journalistic, literary or artistic purposes, provided that: <ul style="list-style-type: none"> (i) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material; (ii) Swinburne Sarawak reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and (iii) Swinburne Sarawak reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.
1.4	<p>Security Principle (<i>Section 9, PDPA</i>)</p>
1.4.1	<p>Swinburne Sarawak shall ensure that personal data is protected by reasonable security safeguards against loss, unauthorised access, misuse, modification and disclosure, through compliance with this policy and procedure and the People, Culture and Integrity Policy.</p>

	<p>1.4.2 If a data processor (e.g. suppliers) processes personal data on behalf of the university, Swinburne Sarawak shall ensure that the data processor:</p> <p>(a) provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and</p> <p>(b) takes reasonable steps to ensure compliance with those measures.</p>
1.5	Retention Principle (<i>Section 10, PDPA</i>)
1.5.1	Swinburne Sarawak shall not keep personal data processed longer than is necessary for the fulfilment of the particular purpose the personal data is collected for.
1.5.2	Swinburne Sarawak shall take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.
1.5.3	Swinburne Sarawak shall ensure that all personal data is retained as per the retention period stated in the Personal Data Register, relevant legislation, or at request of the University management.
1.5.4	In the event the personal data is required to be retained longer than necessary for the purpose for which it was collected for, the management unit must have justification for doing so.
1.6	Data Integrity Principle (<i>Section 11, PDPA</i>)
1.6.1	Swinburne Sarawak shall provide a mechanism to allow a data subject to update and correct his/ her personal data in writing to ensure that the personal data processed or held by Swinburne Sarawak is accurate, complete, not misleading or up-to-date. This includes personal data processed by Swinburne Sarawak but held by a third party.
1.6.2	Swinburne Sarawak shall take reasonable steps to ensure that the source of any personal data is valid and the accuracy of any personal data obtained is maintained in accordance with this policy and procedure, and the People, Culture and Integrity Policy.
1.7	Access Principle (<i>Section 12, PDPA</i>)
1.7.1	<p>Swinburne Sarawak shall allow its data subject to request for access to his/ her personal data and request for corrections if the personal data is inaccurate, incomplete, misleading or not up-to-date unless:</p> <p>(a) Swinburne Sarawak reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or</p> <p>(b) giving access would have an unreasonable impact on the privacy of other individuals; or</p> <p>(c) the request for access is frivolous or vexatious; or</p> <p>(d) the information relates to existing or anticipated legal proceedings between Swinburne Sarawak and the individual, and would not be accessible by the process of discovery in those proceedings; or</p> <p>(e) giving access would reveal the intentions of Swinburne Sarawak in relation to negotiations with the individual in such a way as to prejudice those negotiations; or</p> <p>(f) giving access would be unlawful; or</p> <p>(g) denying access is required or authorised by or under an Malaysian law or a court/ tribunal order; or</p> <p>(h) Swinburne Sarawak has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to Swinburne Sarawak's functions or activities has been, is being or may be engaged in AND giving access would be likely to prejudice the</p>

	<p>taking of appropriate action in relation to the matter; or</p> <p>(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or</p> <p>(j) giving access would reveal evaluative information generated within Swinburne Sarawak in connection with a commercially sensitive decision-making process.</p>
1.7.2	<p>Swinburne Sarawak shall comply with a data access request within twenty-one (21) days from the date of receipt of the data access request.</p> <p>If the request cannot be complied with within twenty-one (21) days, Swinburne Sarawak shall inform the requestor by notice in writing with the reasons why the request cannot be fulfilled within twenty-one (21) days. In this case, Swinburne Sarawak has fourteen (14) additional days to fulfil the access request in whole.</p>
1.7.3	<p>Swinburne Sarawak shall develop guidelines in providing access to the data subject.</p>
1.7.4	<p>Swinburne Sarawak shall ensure all information related to access of data is clearly reflected in the Privacy Collection Notice, including:</p> <p>(a) Any fees for data access request set in accordance with the Personal Data Protection (Fees) Regulations 2013;</p> <p>(b) The methods of obtaining access (e.g. phone, email, etc.);</p> <p>(c) Timeliness of access to be granted upon request (e.g. 21 days via mail); and</p> <p>(d) Clear instructions on how the data subject may request and obtain access to his/ her personal data.</p>
1.7.5	<p>Swinburne Sarawak reserves the right to validate all data access and/ or data update requests by confirming the identity of the data subject through formal identification documentation, such as driver's license, passport and/ or identification card.</p>

SECTION 3 - PROCEDURE

PROCEDURE

	Procedure steps	Responsibility
1.	Implementation of Personal Data Protection Governance Structure	
1.1	Roles and Responsibilities	
	<p>1.1.1 Privacy Officer</p> <ul style="list-style-type: none"> (a) Owner of the Personal Data Protection Governance Structure. (b) Responsible for the administration of the Personal Data Protection Policy and Procedure. (c) Coordinates the implementation of Personal Data Protection Policy and Procedure and any other Personal Data Protection related program. (d) Reviews and updates the Personal Data Protection Policy and Procedure periodically to ensure they are updated with legal requirements, regulations and recommended best practices. (e) Works with all management units within Swinburne Sarawak to ensure that their processes comply with the policy and procedure, and legal requirements of the PDPA. (f) Provides advice and consults all units within Swinburne Sarawak for all matters relating to personal data protection. (g) Represents Swinburne Sarawak as the first point of contact with external parties in relation to personal data protection (e.g. Personal Data Protection Department (<i>Jabatan Perlindungan Data Peribadi</i>)). (h) Conducts compliance monitoring activities in relation to personal data protection. (i) Promotes awareness of personal data protection within Swinburne Sarawak by facilitating activities such as training, information sessions and/or workshops. (j) Cooperates with relevant management units within Swinburne Sarawak, the Commissioner's Office and other legal entities in any incidents, complaints or investigations relating to personal data. 	Privacy Officer
	<p>1.1.2 Head of Management Unit/ Nominee</p> <ul style="list-style-type: none"> (a) Communicates the Privacy Officer's strategic decisions. (b) Becomes point of contact with Swinburne Sarawak staff for all personal data protection matters within Swinburne Sarawak. (c) Ensures that the management unit is aware of the legal requirements of PDPA and that the unit complies with the Personal Data Protection Policy and Procedure. (d) Assists the management unit to resolve any operational inquiries relating to personal data. (e) Coordinates and conducts inquiries and/or investigations for personal data-related issues when necessary and to report 	Head of Management Unit/ Nominee

	Procedure steps	Responsibility
	<p>the findings to the Privacy Officer.</p> <p>(f) Maintains the register of personal data and update it on a regular basis.</p>	
	<p>1.1.3 Swinburne Sarawak staff</p> <p>Process personal data in accordance with all the requirements set out in the Personal Data Protection Policy and Procedure, including not to collect, use or access personal data for own personal use, or for purposes not permitted by the respective job or role, or disclose it to anyone who is not authorised to receive it.</p>	Staff
1.2	Escalation/ reporting channel for personal data protection inquiries and breaches	
	<p>1.2.1 Any suspected violations or complaints shall be reported to the Privacy Officer.</p> <p>1.2.2 In the event of a personal data inquiry or PDPA breach, the following escalation/reporting channel is to be used:</p> <p>(a) Staff to inform relevant Head of Unit/ Nominee; and</p> <p>(b) Heads of Unit/ Nominee to communicate with the Privacy Officer.</p>	Staff, Head of Unit/ Nominee
2	Management of Students' and Student References' Personal and Sensitive Personal Data under PDPA requirements	
2.1	Provision of Notice and Choice (Notice and Choice Principle)	
	<p>2.1.1 Swinburne Sarawak shall notify the students via a written Privacy Collection Notice on its website to ensure that the students are fully aware of and understand the purposes for which their personal data is being processed.</p>	Privacy Officer, M&C
	<p>2.1.2 Swinburne Sarawak shall provide the students with the choice to withdraw their consent from the processing of their personal data for the fulfilment of the contract. Swinburne Sarawak shall explain the implications of not being able to process the personal data if the students choose to withdraw their consent.</p>	
2.2	Consent and Disclosure Management for Processing of Personal and Sensitive Personal Data (Disclosure Principle)	
	<p>2.2.1 The student (including current student, past student, prospective student) is deemed to have given consent for the fulfilment of the contract to provide the student with services and goods he/ she has requested for, as specified in Section 1.1: General Principle of this policy and procedure.</p>	Student
	<p>2.2.2 Swinburne Sarawak shall seek students' consent to process their personal data for purposes other than for the fulfilment of the contract or purposes that have not been specified in the Privacy Collection Notice. The Privacy Collection Notice shall then be updated to reflect the newly identified purposes.</p>	Privacy Officer, M&C
	<p>2.2.3 Swinburne Sarawak shall obtain consent directly from students. However, a relevant person is allowed to provide consent on</p>	M&C, Student Engagement

	Procedure steps	Responsibility
	<p>behalf of the students for the following reasons:</p> <p>(a) In the case of a student who is below the age of eighteen (18) years, the parent, guardian or person who has parental responsibility for the student;</p> <p>(b) In the case of a student who is incapable of managing his/her own affairs, a person who is appointed by a court to manage those affairs, or a person authorised in writing by the student to act on his/ her behalf.</p>	
2.2.4	<p>Swinburne Sarawak may collect and process personal data of student references (e.g. including but not limited to school reference contacts, emergency contacts, spouses, siblings, parents) with whom Swinburne Sarawak does not have a direct commercial transaction/ contractual relationship. Consent is deemed given by this group of student references for the processing and disclosure of the personal data for the fulfilment of the contract with the student.</p> <p>It is the responsibility of the student, who provides the personal data of a reference, to notify the reference (e.g. providing the reference with the Privacy Collection Notice) and obtain the reference's consent.</p>	Student
2.2.5	<p>When processing sensitive personal data:</p> <p>(a) Swinburne Sarawak shall obtain explicit consent from students when processing any sensitive personal data.</p> <p>(b) For new students, Swinburne Sarawak shall obtain explicit consent for the processing of sensitive personal data by requiring students to sign the application form and to take note of the Privacy Collection Notice.</p> <p>(c) For existing students, Swinburne Sarawak shall notify the students about the reasons for processing their sensitive personal data via the Privacy Collection Notice. Existing students are deemed to have given consent; Swinburne Sarawak is not required to obtain explicit consent from existing students.</p>	M&C, Student Engagement
2.3	Consent Management for Direct Marketing Purposes (Disclosure Principle)	
2.3.1	The Director, M&C/ nominee is the owner of the Consent Management for Direct Marketing Process.	M&C
2.3.2	<p>M&C should be the central reference point for any extraction of personal data of the students who provided consent for direct marketing purposes, taking into consideration the specific guiding principles under Section 1.1: General Principle in this policy and procedure.</p> <p>The related management units who use students' personal data for direct marketing purposes should obtain approval from the Director, M&C/ nominee.</p>	M&C
2.3.3	When a student subscribes to a product or service offered by Swinburne Sarawak, Swinburne Sarawak shall allow its	M&C, Student

	Procedure steps	Responsibility
	<p>students to opt-out from direct marketing materials at all times via the following channels:</p> <ul style="list-style-type: none"> (a) Email or write-in to Swinburne Sarawak; or (b) 'Unsubscribe' link in direct marketing emails; or (c) Opt-out option tagged to direct marketing Short Messaging Service (SMS) / Multimedia Messaging Service (MMS). 	
2.3.4	<p>For existing students who have opted-out but would like to opt-in again, students can request to opt-in via email or write-in to Swinburne Sarawak.</p>	M&C, Student
2.3.5	<p>The opt-out/ opt-in-again consent information for direct marketing is captured in the Opt-Out List that may be managed by Swinburne Sarawak or a service provider contracted by Swinburne Sarawak. This information shall be managed as follows:</p> <ul style="list-style-type: none"> (a) The Opt-Out List contains the details of the students who have opted-out from direct marketing activities. In the event where the students would like to opt-in again, their name shall be updated in the Opt-Out List. (b) The Opt-Out List shall be used as the central repository of student consent information for direct marketing and shall be referred to prior to sending out any direct marketing materials to the students. (c) The Director, M&C/ nominee shall have oversight over the usage of the Opt-Out List internally within Swinburne Sarawak in terms of access rights, version controls and any change that would impact the integrity of the list. (d) The Director, M&C/ nominee shall implement an audit trail in the Opt-Out List to capture the last change of consent. The audit trail shall include the date and time of change as well as who performed the change. (e) The purpose of the audit trail is to provide evidence on the latest consent decision made by the students and to exercise the 14-day cooling off period to process the consent information throughout the whole organisation. (f) The cooling off period commences from the date Swinburne Sarawak receives the student request to change consent. (g) In the event of inconsistent consent information, the latest consent information provided by the student based on the audit trail in the system will prevail. 	M&C
2.3.6	<p>When conducting direct marketing activities:</p> <ul style="list-style-type: none"> (a) Management units that perform direct marketing activities shall respect and adhere to students' consent choices and ensure that students who opted-out (in the Opt-Out List) are excluded from any direct marketing activities. (b) If the direct marketing is performed via phone, the representative should ask for the student's consent before the representative communicates the direct marketing message. The phone should be equipped with recording or recalling facility to capture the indication of consent by the student. The indicated choice by the student shall also be 	Staff, M&C

	Procedure steps	Responsibility
	<p>captured in the Opt-Out List.</p> <p>(c) If the direct marketing is done via email, SMS, MMS or snail mail, an opt-out option must be provided.</p>	
2.3.7	<p>Explicit consent is required from student references when using the individual's personal data for direct marketing purposes.</p> <p>Procedure steps 2.3.3 to 2.3.6 shall be applied to student references.</p>	M&C
2.4	Personal Data Security (Security Principle)	
2.4.1	<p>As the processing of personal data is distributed throughout Swinburne Sarawak and personal data can exist in various forms (including electronic data, hardcopy documents, audio files and visual files), when processing students' personal data:</p> <p>(a) every management unit in Swinburne Sarawak shall take practical steps to protect the confidentiality, integrity and availability of the personal data that is processed; and</p> <p>(b) all staff shall take responsibility to protect the personal data by handling personal data in accordance with this policy and procedure, and the People, Culture and Integrity Policy.</p>	Staff
2.5	Personal Data Retention (Retention Principle)	
2.5.1	<p>When retaining the student's personal data:</p> <p>(a) the Head of Management Unit/ nominee shall be responsible for the unit-specific information containing personal data which is created and processed within the management unit;</p> <p>(b) each management unit is responsible for determining the retention period and justification for retaining such information, taking into consideration all the legal and regulatory, contractual and commercial requirements to ensure that the retention period complies with all these requirements;</p> <p>(c) the retention period and the justification for such period shall comply with the retention period stated in the Personal Data Register, relevant legislation, or at request of the University management. ; and</p> <p>(d) each management unit shall ensure secure destruction of information comprising personal data after the retention period according to the retention period stated in the personal data register and guidelines specified in the Management of University Records Policy.</p>	Staff
2.6	Personal Data Integrity (Data Integrity Principle)	
2.6.1	<p>In ensuring integrity of students' personal information:</p> <p>(a) Swinburne Sarawak staff shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date.</p> <p>(b) Swinburne Sarawak staff members, who enter personal data into Swinburne Sarawak's information management systems, shall take precautionary measures to verify the validity of the data with the source to minimise errors and to</p>	Staff

	Procedure steps	Responsibility
	<p>ensure data accuracy.</p> <p>(c) The following measures should be established to achieve data integrity:</p> <p>(i) A mechanism shall be developed to allow students to update and correct their personal data in writing if the students know that the personal data processed or held by Swinburne Sarawak is inaccurate, incomplete, misleading or not up-to-date.</p> <p>(ii) For personal data in electronic format, data integrity should leverage on Swinburne Sarawak's existing information and management practices in regard to data integrity of students and staff's personal data mentioned in the People, Culture and Integrity Policy.</p>	
2.7	Personal Data Access Request Management (Access Principle)	
	<p>2.7.1 In regard to managing personal data access requests:</p> <p>(a) The Director, Student Engagement/ nominee is the owner of the Personal Data Access Request Management Process.</p> <p>(b) Student Engagement represents Swinburne Sarawak as the first point of contact with students for any matters related to PDPA, e.g. personal data access request, personal data correction.</p> <p>(c) Personal data shall be extracted from the student management system as it is deemed to contain the most comprehensive and up-to-date student personal data.</p> <p>(d) The Director, Student Engagement/ nominee shall be responsible for the following:</p> <p>(i) Identify and document the key personal data fields that will be disclosed to the student upon request;</p> <p>(ii) Provide the student with a Personal Data Access Request Form in order for the student to raise a written request for access to personal data;</p> <p>(iii) Decide and document whether a chargeable fee set in accordance with the Personal Data Protection (Fees) Regulations 2013 should be incurred by the student upon receiving the personal data access request in a report form;</p> <p>(iv) Respond to the student's personal data access request within twenty-one (21) days after the request has been made;</p> <p>(v) If the request cannot be fulfilled within twenty-one (21) days, Student Engagement shall notify the student in writing with the reason(s) why the request cannot be fulfilled and respond within another fourteen (14) days.</p>	Student Engagement

	Procedure steps	Responsibility
	<p>2.7.2 In regard to requesting access to personal data and consent information, students may request:</p> <ul style="list-style-type: none"> (a) access to their personal data via email or write-in to Students Operations; or (b) access to their consent information via email or write-in to M&C. <p>If the student finds that the personal data that Swinburne Sarawak processed is inaccurate, incomplete, misleading or not up-to-date, the student shall request for a correction of their personal data by filling in the Amendment to Personal Details Form and submitting it to Student Central.</p>	Student
3	Management of Staff's Personal and Sensitive Personal Data under PDPA requirements	
3.1	<p>In processing personal data of staff, Swinburne Sarawak shall observe the following PDPA requirements:</p> <ul style="list-style-type: none"> (a) Consent is deemed given for the processing of personal data for the performance of the staff contract. (b) The Human Resources Unit is to obtain the staff's or candidates' consent before processing any sensitive personal data. (c) The Human Resources Unit is to notify Swinburne Sarawak staff and candidates about their rights and Swinburne Sarawak's obligation under the PDPA requirements via the Employee's Privacy Collection Notice, Employee Records Policy, Employment Application Form for job applicants. (d) In the event Swinburne Sarawak intends to approach the staff for direct marketing activities and such purpose was not agreed to upon the collection of personal data, explicit consent shall be obtained. (e) The Human Resources Unit shall provide notification to the staff on how Swinburne Sarawak processes and discloses their personal data. (f) The Human Resources Unit shall allow staff access to their personal data/ sensitive personal data via hardcopy employee profiles in physical files, electronic payroll information and/ or claims information. (g) Human Resources Unit shall allow request by staff for correction of the personal data that is inaccurate, incomplete, misleading or not up-to-date. 	Human Resources Unit
4	Management of Third Party Suppliers' Personal and Sensitive Personal Data under PDPA requirements	
4.1	<p>Swinburne Sarawak's Finance Unit shall develop a Personal Data Protection clause that addresses the following points:</p> <ul style="list-style-type: none"> (a) Suppliers to comply with the PDPA; (b) Suppliers to take reasonable steps to implement technical and organisational security measures to ensure the protection of personal data and sensitive personal data; (c) Suppliers to provide assistance to Swinburne Sarawak to comply with the rights of data subjects; (d) Suppliers to ensure that their subcontractors process the personal 	Finance Unit, Head of Management Unit/ Nominee

	Procedure steps	Responsibility
	<p>data in accordance with the PDPA;</p> <p>(e) Before submitting any personal data to Swinburne Sarawak, suppliers shall obtain the consent of the data subjects and notify them upon the collection of the data that the data is disclosed to Swinburne Sarawak for fulfilment of the contract;</p> <p>(f) Swinburne Sarawak agrees to comply with the PDPA requirements to the personal data received from the suppliers;</p> <p>(g) Suppliers to note Swinburne Sarawak's Privacy Collection Notice and to declare that the personal data provided is accurate, complete and up-to-date.</p> <p>For any contract or agreement with a third party supplier in a commercial transaction, the respective management units and Swinburne Sarawak's Finance Unit shall ensure that this clause is inserted into the contract or agreement to address the PDPA requirements.</p>	
4.2	This Personal Data Protection clause for third parties shall be included in all renewal of contracts with third party service suppliers in a commercial transaction with Swinburne Sarawak.	Staff
4.3	In the event Swinburne Sarawak intends to approach the third party service supplier's data subject for direct marketing activities, explicit consent shall be obtained from the individual.	
5	Management and Use of Closed Circuit Television (CCTV) under Advisory Guidelines to the PDPA	
5.1	CCTVs are installed and managed in Swinburne Sarawak for safety and security purposes, in accordance with the University's CCTV Policy and Procedure.	Facilities & Services Unit
5.2	Explicit consent shall be obtained from individuals if the CCTV recordings are to be used for a commercial transaction, such as for promotion or sale of products and services.	Manager, Facilities & Services/ nominee

SUPPORTING DOCUMENTATION

Forms and Records Management

Form	Retention Time	Retention Location
Amendment to Personal Details Form		http://www.swinburne.edu.my/student_operations/forms/Personal_Details_Amend%202015%20v4(4)%20Final%2002072015.pdf
Personal Data Access Request Form		The form is available at two locations: http://www.swinburne.edu.my/student_operations/forms/Personal%20Data%20Access%20Form.pdf http://swinburne.edu.my/privacy/docs/Personal%20Data%20Access%20Form.pdf

Related Material

Name	Location	Document Type
Closed Circuit Television (CCTV) Policy	Staff/ Policies and Regulations Directory/ Management Unit Manuals/ Facilities and Services Manual/ CCTV Policy & Procedures	Policy
Consent Management for Direct Marketing	Staff/ Policies and Regulations Directory/ University Governance/Personal Data Protection Policy & Procedures/Unit Rule	Unit Rule
Employee Records Policy	Staff/ Policies and Regulations Directory/ Management Unit Manuals/ Human Resources Manual/ Employee Records Policy & Procedures	Policy
Management of University Records	Staff/ Policies and Regulations Directory/ University Governance/ Management of University Records Policy & Procedures	Policy
People, Culture and Integrity Policy	http://www.swinburne.edu.au/policies/hr/index.html	Policy
Employee's Privacy Collection Notice	Blackboard/My.Swinburne/Policies and Regulations Directory/Management Unit Manuals/Human Resources Manual/Employee Records/ Data Privacy/Employee Records Policy & Procedures/Related Materials/Employee's Privacy Collection Notice	Notice
Privacy Collection Notice (Students & Suppliers)	http://www.swinburne.edu.my/privacy/	Notice
Students' Personal Data Access and Correction Request Management	Staff/ Policies and Regulations Directory/ University Governance/Personal Data Protection Policy & Procedures/Unit Rule	Unit Rule
Proposal Paper [No. 1/2014]	http://www.pdp.gov.my/images/pdf_folder/COMBINED%20PDF%20Direct%20Marketing%20Guideline-BM-3.pdf "Guide in Dealing with Direct Marketing Under Personal Data Protection Act (PDPA) 2010" <i>This document provides guidelines on dealing with advertising or marketing material that is directed to a particular individual under PDPA law.</i>	Proposal Paper

Name	Location	Document Type
Proposal Paper [No. 2/2014]	http://www.pdp.gov.my/images/pdf_folder/COMPLIANCEkert asrundingan-combined.pdf “Guideline on Compliance of Personal Data Protection Act (PDPA) 2010” <i>This document provides guidelines that can be used by organisations to comply with the Act.</i>	
Proposal Paper [No. 3/2014]	http://www.pdp.gov.my/images/pdf_folder/EMPLOYER-EMPLOYEE.pdf “Guide on the Management of Employee Data Under Personal Data Protection Act (PDPA) 2010” <i>This document provides guidance on dealing with personal data of an employee by following the seven Principles of PDPA.</i>	
Proposal Paper [No. 4/2014]	http://www.pdp.gov.my/images/pdf_folder/kertas_rundingan_ awam /BIL_4 KEPERLUAN PERSETUJUAN-ENG.pdf “Advisory Guidelines Related to Consent Requirement under the Personal Data Protection Act (PDPA) 2010” <i>This document provides practical guidance for data users in obtaining consent in order to satisfy the requirements for processing personal data under PDPA.</i>	
Proposal Paper [No. 5/2014]	http://www.pdp.gov.my/images/pdf_folder/kertas_rundingan_ awam /CCTV ENG-09062014.pdf “Guide on the Management of CCTV Under Personal Data Protection Act (PDPA) 2010” <i>This document provides guidelines for organisations in managing the CCTV under PDPA.</i>	

SECTION 4 - GOVERNANCE

RESPONSIBILITY

Policy Owner	Privacy Officer
---------------------	-----------------

VERSION CONTROL AND CHANGE HISTORY

Version Number	Approval Date	Approved by	Amendment
3	11 April 2017	Board of Directors	Changes made to address audit findings by the Department of Personal Data Protection.
2	1 September 2015	Board of Directors	Inclusion of current processes in place to support the University’s compliance with the PDPA 2010.
1	22 January 2015	Board of Directors	New policy and procedure

POLICIES & REGULATIONS DIRECTORY REQUIREMENTS

CATEGORY

Personal Data Protection

KEYWORDS

PDPA, Privacy, Personal Data