

## DURBAN UNIVERSITY OF TECHNOLOGY

### PRIVACY AND PROTECTION OF PERSONAL INFORMATION POLICY

<b>Document name</b>	Privacy and Protection of Personal Information Policy
<b>Document Owner</b>	Vice-Chancellor (Information Officer)
<b>Operational Manager</b>	Senior and Executive Management
<b>Contact and telephone number for support</b>	<a href="mailto:Karenl@dut.ac.za">Karenl@dut.ac.za</a> <a href="mailto:popia@dut.ac.za">popia@dut.ac.za</a>
<b>Status</b>	Approved
<b>Approved by</b>	Council
<b>Date approved</b>	25 November 2023
<b>Date last amended</b>	
<b>Title of manager responsible for monitoring policy implementation</b>	DVC: Research, Innovation and Engagement, DVC: Teaching and Learning, Registrar (Deputy Information Officers).
<b>Review date</b>	<b>2026</b>

#### Related documents

<p><b>DUT documents</b> (e.g. Policies, Regulations, Guidelines, Contracts)</p> <ul style="list-style-type: none"> <li>• <b>DUT Statute</b></li> <li>• <b>ENVISION 2030</b></li> <li>• <b>Student Records Policy</b></li> <li>• <b>Data Governance Charter</b></li> <li>• <b>Information and Data Governance Asset Register</b></li> </ul>	<p><b>Other</b> (e.g. Legislation, DHET, national and international standards and directives, national regulations and guidelines)</p> <ul style="list-style-type: none"> <li>• The Higher Education Act 101 of 1997 (as amended);</li> <li>• The Promotion of Access to Information Act 2 of 2000;</li> <li>• The Consumer Protection Act 68 of 2008;</li> <li>• The Companies Act 71 of 2008 (as amended);</li> <li>• The Close Corporations Act 69 of 1984 (as amended);</li> <li>• Electronic Communications and Transactions Act 25 of 2002;</li> <li>• Magistrate Court Act 59 of 1944 (as amended);</li> <li>• Supreme Court Act 59 of 1959;</li> <li>• Arbitration Act 42 of 1965;</li> <li>• Intellectual Property Laws Amendment Act 38 of 1997;</li> <li>• Intellectual Property Rights from Publicly Financed ; Research and Development Act 51 of 2008 and</li> </ul>
--	--

	<p>Regulations;</p> <ul style="list-style-type: none"> <li>• All applicable intellectual property legislation not specifically mentioned in this document</li> <li>• Copyright Act 98 of 1978</li> <li>• King III</li> <li>• Codes of Conduct issued by Regulator and/or Parliament into any relevant Act from time to time</li> <li>• Protection of Personal Information Act 4 of 2013;</li> <li>• The Constitution of the Republic of South Africa.</li> </ul>
<b>Structures affected by this policy</b>	<ul style="list-style-type: none"> <li>• EMC</li> <li>• Data Governance Committee</li> <li>• Executive Deans</li> <li>• Directors</li> <li>• Heads of Academic Departments</li> <li>• All Service Departments</li> <li>• All other Contract Owners</li> </ul>
<b>Website address of this document:</b>	<b>Public website</b>
<b>Acknowledgement</b>	The University of Johannesburg is acknowledged for granting permission to use their Policy: Privacy and Protection of Personal Information.

## TABLE OF CONTENTS

1.	<b>Preamble</b>	4
2.	<b>Purpose</b>	4
3.	<b>Scope</b>	4
4.	<b>Definitions And Abbreviations</b>	5
5.	<b>Rights Of Data Subjects</b>	6
6.	<b>Lawful Processing</b>	6
7.	<b>Minimality</b>	6
8.	<b>Consent</b>	7
9.	<b>Collection Of Personal Information</b>	7
10.	<b>Specific Purpose</b>	8
11.	<b>Retention and Restriction of Records</b>	8
12.	<b>Further Processing</b>	8
13.	<b>Quality Of Information</b>	9
14.	<b>Notification Of Collection</b>	9
15.	<b>Security And Integrity</b>	10
16.	<b>Notification Of Security Compromises</b>	11
17.	<b>Access To Personal Information</b>	11
18.	<b>Correction Of Personal Information</b>	12
19.	<b>Special Personal Information</b>	12
20.	<b>Personal Information Of Children</b>	12
21.	<b>Transfers Of Personal Information Outside Republic</b>	13

## **I. PREAMBLE**

- 1.1 The Durban University of Technology is committed to protecting all persons' privacy and recognises that it needs to comply with statutory requirements whenever it collects, processes and distributes personal information. The Constitution of the Republic of South Africa provides that everyone has the right to privacy and the Protection of Personal Information Act 4 of 2013 enforces the right to protection against unlawful collection, retention, dissemination and use of personal information.
- 1.2 The Durban University of Technology, is established, mandated and governed by the Higher Education Act 101 of 1997 (as amended) and its Institutional Statute. In order to perform its functions, the University needs to process personal information about all persons with which it deals and interacts with from time to time. There are various reasons why the University may need to process such information, such as monitoring of performance, achievements, health and safety of students, employees or other stakeholders. The University may also be obligated by Law or governing bodies to process such information for reporting, statistical or other purposes.
- 1.3 The Durban University of Technology strives to balance the right to privacy with other competing rights, such as the right to access to information and the free flow of information.

## **2. PURPOSE**

- 2.1 The purpose of this policy is to demonstrate the University's commitment to safeguarding personal information of all persons, including juristic persons, with who it interacts and to ensure that the University and its employees comply with the requirements imposed by the Protection of Personal Information Act 4 of 2013.
- 2.2 Without limiting the generality of the aforementioned purpose, the further purposes are to:
  - 2.2.1 establish an institution-wide policy that will provide direction with respect to the manner of compliance with the Protection of Personal Information Act 4 of 2013;
  - 2.2.2 give effect to the right to privacy and at the same time balance the right to privacy against other rights such as the right to access to information, and to protect important interests such as the free flow of information;
  - 2.2.3 regulate the manner in which personal information may be processed;
  - 2.2.4 establish measures to ensure respect for and to promote, enforce and fulfil the rights protected.

## **3. SCOPE**

- 3.1 This policy has institution-wide application.
- 3.2 This policy applies to personal information collected by the University in connection with the services it offers. This includes information collected offline through our Helplines and call centres, and online through our websites, branded pages on third party platforms and applications accessed or used through such websites or third party platforms which are operated by or on behalf of the University. This policy is hereby incorporated into and forms part of the terms and conditions of use of the applicable University sites.
- 3.3 This policy does not apply to:
  - 3.3.1 information collected by third party websites, platforms and/or applications ("Third Party Sites") which we do not control;

- 3.3.2 information collected by Third Party Sites which you access via links on University sites; or  
3.3.3 banners, sweepstakes and other advertisements or promotions on Third Party Sites that we may sponsor or participate in.

#### 4. **DEFINITIONS AND ABBREVIATIONS**

- 4.1 **“Act”** means the Protection of Personal Information Act 4 of 2014.
- 4.2 **“CCTV”** means closed circuit television.
- 4.3 **“Consent”** means any voluntary, specific and informed expression agreeing to the processing of personal information.
- 4.4 **“Data Subject”** means the person to whom the personal information relates and in relation to the University, data subject would include students, employees, prospective students; applicants; alumni; research participants; employees; employment candidates; visitors; members of the public and any other individual with whom the University may interact from time to time, whether or not such person is a natural person or a juristic person.
- 4.5 **“De-identify”** in relation to personal information of a data subject means to delete information that –
- (a) identifies the data subject;
  - (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
  - (c) can be linked by a reasonable foreseeable method or other information that identifies a data subject,
- and **“de-identified”** has a corresponding meaning”.
- 4.6 **“Personal Information”** as defined in POPIA, means information relating to an identifiable, living individual or identifiable, existing company, including, but not limited to:
- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
  - information relating to the education or the medical, financial, criminal or employment history of the person;
  - any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - the biometric information of the person;
  - the personal opinions, views or preferences of the person;
  - correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  - the views or opinions of another individual about the person; and  
the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person
- 4.7 **“PAIA”** means the Promotion of Access to Information Act.
- 4.8 **“Policy”** means this Privacy and Protection of Personal Information Policy.
- 4.9 **“POPI”** means the Protection of Personal Information Act.
- “Processing”** as defined in POPIA means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information including:
- the collection, receipt, recording, organisation, collation, storage, updating or modification,

retrieval, alteration, consultation or use;

- disseminations by means of transmission, distribution, or making available in any other form; or
- merging, linking, as well as restriction, degradation, erasure, or destruction of information.

4.10 **“Record”** means any recorded personal information, regardless of its form or medium, including any writing, electronic information, label, marking, image, film, map, graph, drawing, tape and that is in the possession or under the control of a responsible party, irrespective of whether it has been created by the responsible party or not and regardless of when it came into existence.

4.11 **“Responsible party”** means, the Durban University of Technology, who engages in the act of processing personal information.

4.12 **“Special Personal Information”** means any information that could be used to identify a data subject and includes -

(a) Religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, DNA, sexual life and criminal behaviour.

(b) Personal information concerning a child.

4.13 **“University”** means the Durban University of Technology, which includes its faculties, departments, companies, bodies, organisations and employees.

## **5. RIGHTS OF DATA SUBJECTS**

5.1 The University respects a data subject’s right to have his, her or its personal information processed lawfully.

5.2 Data subjects have the right to:

5.2.1 be notified that personal information about him, her or it is being collected or that his, her or its personal information has been accessed or acquired by an unauthorised person;

5.2.2 to establish whether the University holds personal information of that data subject and to request access thereto;

5.2.3 to request, where necessary, the correction, destruction or deletion of his, her or its personal information;

5.2.4 to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information;

5.2.5 to object to the processing of his, her or its personal information at any time for purposes of direct marketing;

5.2.6 not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person;

5.2.7 to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information;

5.2.8 to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

## **6. LAWFUL PROCESSING**

6.1 The University processes personal information lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

## **7. MINIMALITY**

7.1 Only information which is necessary for the specific purpose for which it is collected, is

processed.

7.2 Information which is collected is adequate, relevant and not excessive.

7.3 Information is collected in a manner which does not infringe the rights of the data subject.

## **8. CONSENT**

8.1 The University only processes personal information with the express consent of the data subject or a competent person where the data subject is a child.

8.2 The University processes personal information without express written consent, if:  
8.2.1 processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

8.2.2 processing complies with an obligation imposed by law on the University;

8.2.3 processing protects a legitimate interest of the data subject;

8.2.4 processing is necessary for the proper performance of a public law duty by the University; or

8.2.5 processing is necessary for pursuing the legitimate interests of the University or of a third party to whom the information is supplied.

8.3 The data subject or competent person may withdraw his, her or its consent, at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information will not be affected.

8.4 A data subject may object, at any time, to the processing of personal information in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

8.5 If a data subject has objected to the processing of personal information the University no longer processes the personal information and the relationship between the University and the data subject may be terminated.

## **9. COLLECTION OF PERSONAL INFORMATION**

9.1 The University collects personal information from the data subject directly, except as otherwise provided for below.

9.2 The University collects personal information from other sources other than the data subject directly if:

9.2.1 the information is contained in or derived from a public record or has deliberately been made public by the data subject;

9.2.2 the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;

9.2.3 collection of the information from another source would not prejudice a legitimate interest of the data subject;

9.2.4 collection of the information from another source is necessary:

9.2.4.1 to avoid prejudice to the maintenance of the law by the University, including the prevention, detection, investigation, prosecution and punishment of offences;

9.2.4.2 to comply with an obligation imposed by law or to enforce legislation;

9.2.4.3 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

9.2.4.4 in the interests of national security; or

9.2.4.5 to maintain the legitimate interests of the University or of a third party to whom the information is supplied;

9.2.5 compliance would prejudice a lawful purpose of the collection; or

9.2.6 compliance is not reasonably practicable in the circumstances of the particular case.

## **10. SPECIFIC PURPOSE**

10.1 The University collects personal information for a specific, explicitly defined and lawful purpose related to a function or activity of the University.

10.2 The University takes steps to ensure that the data subject is aware of the purpose of the collection of the information.

## **11. RETENTION AND RESTRICTION OF RECORDS**

11.1 The University does not retain records of personal information any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

11.1.1 retention of the record is required or authorised by law;

11.1.2 the University reasonably requires the record for lawful purposes related to its functions or activities;

11.1.3 retention of the record is required by a contract between the parties thereto; or

11.1.4 the data subject or a competent person where the data subject is a child has consented to the retention of the record.

11.2 Records of personal information may be retained for periods in excess of those contemplated 11.1 for historical, statistical or research purposes and the University ensures appropriate safeguards against the records being used for any other purposes.

11.3 Whenever the University uses a record of personal information of a data subject to make a decision about the data subject, the University:

11.3.1 retains the record for such period as may be required or prescribed by law or retains the record for a period which affords the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

11.4 The University destroys or deletes a record of personal information or de-identify it as soon as reasonably practicable after the University is no longer authorised to retain the record.

11.5 The destruction or deletion of a record of personal information is done in a manner that prevents its reconstruction in an intelligible form.

11.6 The University restricts processing of personal information if:

11.6.1 its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;

11.6.2 the University no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

11.6.3 the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

11.6.4 the data subject requests to transmit the personal data into another automated processing system.

## **12. FURTHER PROCESSING**

12.1 Further processing of personal information is done in accordance or compatible with the purpose for which it was collected initially.

12.2 To assess whether further processing is compatible with the purpose of collection, the University takes account of:



- 12.2.1 the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
- 12.2.2 the nature of the information concerned;
- 12.2.3 the consequences of the intended further processing for the data subject;
- 12.2.4 the manner in which the information has been collected; and
- 12.2.5 any contractual rights and obligations between the University and the data subject.
- 12.3 The further processing of personal information is not incompatible with the purpose of collection if:
  - 12.3.1 the data subject or a competent person where the data subject is a child has consented to the further processing of the information;
  - 12.3.2 the information is available in or derived from a public record or has deliberately been made public by the data subject;
  - 12.3.3 further processing is necessary:
    - 12.3.3.1 to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
    - 12.3.3.2 to comply with an obligation imposed by law;
    - 12.3.3.3 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
    - 12.3.3.4 in the interests of national security;
  - 12.3.4 the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:
    - 12.3.4.1 public health or public safety; or
    - 12.3.4.2 the life or health of the data subject or another individual;
    - 12.3.4.3 the information is used for historical, statistical or research purposes and the University ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
    - 12.3.4.4 the processing is exempted by the Protection of Personal Information Act 4 of 2013.

### **13. QUALITY OF INFORMATION**

- 13.1 The University takes reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which personal information is collected or further processed.

### **14. NOTIFICATION OF COLLECTION**

- 14.1 Whenever the University collects personal information it takes reasonably practicable steps to ensure that the data subject is aware of:
  - 14.1.1 the information being collected and where the information is not collected from the data subject, the source from which it is collected;
  - 14.1.2 the name and address of the University's Information Officer;
  - 14.1.3 the purpose for which the information is being collected;
  - 14.1.4 whether or not the supply of the information by that data subject is voluntary or mandatory;
  - 14.1.5 the consequences of failure to provide the information;
  - 14.1.6 any particular law authorising or requiring the collection of the information;
  - 14.1.7 the fact that, where applicable, the University intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

- 14.1.8 any further information such as the:
  - 14.1.8.1 recipient or category of recipients of the information;
  - 14.1.8.2 nature or category of the information;
  - 14.1.8.3 existence of the right of access to and the right to rectify the information collected;
  - 14.1.8.4 the existence of the right to object to the processing of personal information; and
  - 14.1.8.5 right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator.
- 14.2 The steps referred to in 14.1 is taken:
  - 14.2.1 if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or
  - 14.2.2 in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.
- 14.3 The University does need not comply with 14.1 if:
  - 14.3.1 the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;
  - 14.3.2 non-compliance would not prejudice the legitimate interests of the data subject;
  - 14.3.3 non-compliance is necessary:
    - 14.3.3.1 to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
    - 14.3.3.2 to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
    - 14.3.3.3 for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or
    - 14.3.3.4 in the interests of national security;
  - 14.3.4 compliance would prejudice a lawful purpose of the collection;
  - 14.3.5 compliance is not reasonably practicable in the circumstances of the particular case; or
  - 14.3.6 the information will:
    - 14.3.6.1 not be used in a form in which the data subject may be identified; or
    - 14.3.6.2 be used for historical, statistical or research purposes.

## **15. SECURITY AND INTEGRITY**

- 15.1 The University aims and strives to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:
  - 15.1.1 loss of, damage to or unauthorised destruction of personal information; and
  - 15.1.2 unlawful access to or processing of personal information.
- 15.2 It is the objective of the University to take reasonable measures to:
  - 15.2.1 identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
  - 15.2.2 establish and maintain appropriate safeguards against the risks identified;
  - 15.2.3 regularly verify that the safeguards are effectively implemented; and
  - 15.2.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- 15.3 Anyone processing personal information on behalf of the University:

- 15.3.1 processes such information only with the knowledge or authorisation of the University; and
- 15.3.2 treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.
  
- 15.4 The University ensures, by way of written contracts between the University and an operator, that the operator which processes personal information for the University establishes and maintains the sufficient and proper security measures as required by the Act.

## **16. NOTIFICATION OF SECURITY BREACHES**

- 16.1 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the University notifies the Regulator and the data subject - unless the identity of such data subject cannot be established - as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.
- 16.2 The University only delays notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.
- 16.3 The University notifies the data subject by way of written notification:
  - 16.3.1 Mailed to the data subject's last known physical or postal address;
  - 16.3.2 sent by e-mail to the data subject's last known e-mail address;
  - 16.3.3 placed in a prominent position on the website of the responsible party;
  - 16.3.4 published in the news media; or
  - 16.3.5 as may be directed by the Regulator.
- 16.4 The notification provides sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:
  - 16.4.1 a description of the possible consequences of the security compromise;
  - 16.4.2 a description of the measures that the responsible party intends to take or has taken to address the security compromise;
  - 16.4.3 a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
  - 16.4.4 if known to the University, the identity of the unauthorised person who may have accessed or acquired the personal information.

## **17. ACCESS TO PERSONAL INFORMATION**

- 17.1 A data subject, having provided adequate proof of identity, has the right to:
  - 17.1.1 request the University to confirm, free of charge, whether or not the University holds personal information about the data subject; and
  - 17.1.2 request from the University the record or a description of the personal information about the data subject held by the University, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information;
- 17.2 The University issues the record to the data subject:

- 17.2.1 within a reasonable time;
- 17.2.2 at a prescribed fee, if any, together with the written estimate of the fee before providing the services;
- 17.2.3 in a reasonable manner and format; and
- 17.2.4 in a form that is generally understandable.

## **18. CORRECTION OF PERSONAL INFORMATION**

- 18.1 A data subject may, in the prescribed manner, request the University to:
  - 18.1.1 correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
  - 18.1.2 destroy or delete a record of personal information about the data subject that the University is no longer authorised to retain.
- 18.2 On receipt of a request the University, as soon as reasonably practicable:
  - 18.2.1 corrects the information;
  - 18.2.2 destroys or deletes the information;
  - 18.2.3 provide the data subject, with credible evidence in support of the information; or
  - 18.2.4 where agreement cannot be reached between the University and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

## **19. SPECIAL PERSONAL INFORMATION**

- 19.1 The University, subject to 19.2.1 to 19.2.5, does not process special personal information concerning:
  - 19.1.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
  - 19.1.2 the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
- 19.2 The University, processes special personal information concerning:
  - 19.2.1 processing is carried out with the consent of a data subject;
  - 19.2.2 processing is necessary for the establishment, exercise or defence of a right or obligation in law;
  - 19.2.3 processing is necessary to comply with an obligation of international public law;
  - 19.2.4 processing is for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;
  - 19.2.5 information has deliberately been made public by the data subject.

## **20. PERSONAL INFORMATION OF CHILDREN**

- 20.1 The University processes personal information of children:

- 20.1.1 with the prior consent of a competent person;
- 20.1.2 where it is necessary for the establishment, exercise or defence of a right or obligation in law;
- 20.1.3 where it is necessary to comply with an obligation of international public law;
- 20.1.4 where it is necessary for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- 20.1.5 which has deliberately been made public by the child with the consent of a competent person.

## **21. TRANSFERS OF PERSONAL INFORMATION OUTSIDE REPUBLIC**

- 21.1 The University does not transfer personal information about a data subject to a third party who is in a foreign country unless:
  - 21.1.1 the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
  - 21.1.2 the data subject consents to the transfer;
  - 21.1.3 the transfer is necessary for the performance of a contract between the data subject and the University, or for the implementation of pre-contractual measures taken in response to the data subject's request;
  - 21.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the University and a third party; or
  - 21.1.5 the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject to that transfer; and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.