

DEPARTMENT OF HIGHER EDUCATION AND TRAINING INFORMATION STANDARD

DHET 011

DATA CONFIDENTIALITY STANDARD

05 JULY 2023



higher education  
& training

Department:  
Higher Education and Training  
REPUBLIC OF SOUTH AFRICA

Information Systems Management  
Department of Higher Education and Training  
Private Bag X174  
PRETORIA  
0001

Point of contact:  
HETIS Officer  
Telephone: 012 312 6191/5965  
E-mail: HETIS.Officer@dhet.gov.za

<b>Table of Contents</b>	<b>Page</b>
1. List of acronyms and abbreviations.....	3
2. Glossary .....	4
3. Background .....	6
4. Purpose of the standard .....	7
5. Data confidentiality .....	7
6. Legislative Framework.....	9
7. Lawful conditions .....	10
8. Applicability .....	12
9. Disseminated data .....	12
10. Conditions of handling data .....	13
11. Sharing of confidential data with a third party .....	13
12. Breach of confidentiality.....	13
13. Bibliography.....	15
14. Appendix 1 –Confidentiality Declaration Form for Departmental staff.....	16
15. Appendix 2 – Confidentiality Declaration Form for external organisations and entities of the Department .....	17

## 1. List of acronyms and abbreviations

AATTCs	Accredited Artisan Trade Test Centres
CAS	Central Application System
CETCs	Community Education and Training colleges
DBE	Department of Basic Education
DHET	Department of Higher Education and Training
HEIs	Higher Education Institutions
HETIS	Higher Education and Training Information System
PSETIP	Post-School Education and Training Information Policy
MIS	Management Information System
NAMB	National Artisan Moderation Body
NSFAS	National Student Financial Aid Scheme
PERSAL	Personnel and Salary System
POPI	Protection of Personal Information
POPIA	Protection of Personal Information Act
PSET	Post-School Education and Training
SASQAF	South African Statistical Quality Assessment Framework
SDPs	Skills Development Providers
SETAs	Sector Education and Training Authorities
TVET	Technical and Vocational Education and Training

## 2. Glossary

<b>Confidential data</b>	information obtained by a person on the understanding that they will not disclose it to others, or obtained in circumstances where it is expected that they will not disclose it.
<b>Data Confidentiality</b>	A property of data, usually resulting from legislative measures, which prevents it from unauthorised disclosure.
<b>Data</b>	a representation of facts, concepts, or instructions in a formal manner, suitable for communication, interpretation, or processing by humans or by automatic means.
<b>Data Manager</b>	any person who manages an administrative process by which the required data is acquired, validated, stored, protected, and processed, and by which its accessibility, reliability, and timeliness is ensured to satisfy the needs of the data users.
<b>Data subject</b>	the person to whom personal information relates. This includes students, customers, employees, suppliers, contractors, vendors, third parties and stakeholders.
<b>Biometrics</b>	a technique of personal identification that is based on fingerprinting.
<b>HETIS Officer</b>	an official charged with certain responsibilities regarding post-school education and training information in terms of the Post-School Education and Training Information Policy of 2019.
<b>Personal information</b>	information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person including, but not limited to identifying number, demographic information, medical information and contact details.
<b>Post-School Education and Training Institutions</b>	education and training institutions that include universities, national institutes of higher education and private higher education institutions, technical and vocational education and training colleges, private colleges, community education and training colleges, and skills development providers. These are established, declared or registered by any law assigned to the Minister of Higher Education, Science and Innovation.
<b>Responsible Party</b>	person which alone or in conjunction with others, determines the purpose of and means for processing personal information.
<b>Processing</b>	the operation performed on data in order to derive new information according to a given set of rules.

<b>Statistics</b>	aggregated numerical information relating to demographic, economic, financial, environmental, social, or similar matter, at national, provincial or local level, which is compiled and analysed according to relevant scientific and statistical methodology.
<b>Third party</b>	someone other than the data subject, controller, processor and persons with authority of the controller or processor to process the data.

### 3. Background

- 3.1 Students and staff in Post-School Education and Training (PSET) institutions, namely public and registered private Higher Education Institutions (HEIs), Technical and Vocational Education and Training (TVET) colleges, Community Education and Training colleges (CETCs) and registered private colleges, submit their personal information to their relevant Post-School Education and Training (PSET) institutions as part of enrolment, registration and personnel management processes.
- 3.2 Similarly, students and learners submit their personal information to Sector Education and Training Authorities (SETAs), National Artisan Moderation Body, Accredited Artisan Trade Test Centres (AATTCs) and Skills Development Providers (SDPs), as part of their registration processes for learnerships, skills programmes, apprenticeships and internships.
- 3.3 The above-mentioned institutions and providers, in turn, upload/provide individual records of students, learners and staff to the Department of Higher Education and Training (hereafter referred to as the Department), which are uploaded/captured on the Management Information System (MIS) according to a submission schedule provided by the Department.
- 3.4 The Department also has records of students who have applied for and have been granted National Student Financial Aid Scheme (NSFAS) study loans/bursaries. Employers' information is also uploaded by the SETAs on the Department's MIS.
- 3.5 The Department, therefore, manages a large number of unit records of institutional, student, learner, staff and employer data from PSET institutions, SETAs, ATTCs, SDPs and NSFAS.
- 3.6 The Department processes the collected data to produce an annual statistics report on PSET which serves as an important resource for planning, allocation of budgetary resources, monitoring and reporting purposes to inform policy and decision-making. The collected data is also used to respond to special data requests sent to the Department by users.
- 3.7 PSET institutions, ATTCs, SDPs and SETAs providing data to the Department, therefore, need to be assured that their data are kept confidential in line with the existing national policy and legislation that regulates matters concerning the confidentiality of personal data.
- 3.8 The Department also keeps individual records of its staff members in the Personnel and Salary System (PERSAL) and finance system, and Departmental employees need to be assured that their personal information is kept confidential.

- 3.9 Personal information data from the Department of Basic Education (DBE) is also acquired by the Department for the purposes of updating the Central Application System (CAS) database, and any relevant analysis that the Department may need to conduct using DBE data. The Department has an MoU with DBE in this regard, and it is our responsibility to ensure safeguarding the data from DBE.
- 3.10 The following sections outline the purpose of the standard, the legal framework which governs the conditions under which confidential data must be managed and disseminated, and the measures to be undertaken in the event of a breach of confidentiality.

#### **4. Purpose of the standard**

- 4.1 The purpose of this standard is to ensure that the Department secures the confidentiality of personal data that it collects, processes, quality assures, analyses and disseminates. Personal data of officials in the Department must also be kept confidential (this includes data on PERSAL, finance and biometrics).
- 4.2 It directs Departmental staff who access, process, analyse and disseminate data on the measures that need to be undertaken to protect confidential data, and stipulates the processes that the Department must follow in the event of breach of confidentiality.
- 4.3 This standard also sets out the conditions under which confidential data could be shared with third parties.

#### **5. Data confidentiality**

- 5.1 According to the Concepts and Definitions for Statistics South Africa, data confidentiality refers to “a property of data, usually resulting from legislative measures, which prevents it from unauthorised disclosure”<sup>1</sup>.
- 5.2 Personal data referred to in this standard includes, but are not limited to the following examples:
- 5.2.1 Name, such as full name, maiden name, mother’s maiden name, or alias;
- 5.2.2 Personal identification numbers;

---

<sup>1</sup> Statistics South Africa, Concepts and Definitions for Statistics South Africa, 2017

- 5.2.3 Address information, such as physical address, email address;
- 5.2.4 Biometrics of the person;
- 5.2.5 Telephone or cell phone numbers; and
- 5.2.6 Bank account details.
- 5.3 Section 11(1) (a) of the Protection of Personal Information (POPI) Act<sup>2</sup> stipulates that “personal information may only be processed if the data subject or a competent person<sup>3</sup> where the data subject is a child<sup>4</sup> consents to the processing”.
- 5.4 The Department must ensure that institutions and entities collecting data from students, learners and staff for further processing obtain consent from affected individuals. Statements of consent may be standardised for different PSET sectors.
- 5.5 Where the collection and/processing of data involves other organisations, the relevant Departmental Directorate must ensure that the receiving organisation has policies and protocols on data confidentiality in place, to ensure that data confidentiality will not be compromised during processing and dissemination.
- 5.6 Access to confidential data obtained by the Department from its institutions and entities is limited to authorised Departmental data managers and officials responsible for the collection, processing, quality assurance, analysing and dissemination of data. Service providers who are involved in the development and/ maintenance of information systems, as well as those involved in undertaking data audits will also have access to confidential and personal information data.
- 5.7 All Departmental staff responsible for the collection, processing, analysing, dissemination and archiving of data, as well as auditors who might require access to confidential data must sign a declaration form (**Appendix 1**), confirming that they recognise their responsibilities and agree to preserve the confidentiality of personal data in their possession.

---

<sup>2</sup> Protection of Personal Information Act (Act No. 4 of 2013).

<sup>3</sup> “competent person” means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

<sup>4</sup> “child” means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

- 5.8 The declaration form will also be signed by service providers who might have access to confidential data when developing and/maintaining information systems for the Department **(Appendix 2)**.
- 5.9 The Data Confidentiality Standard must be read in conjunction with the Data Dissemination Standard of the Department of Higher Education and Training (DHET, 2021)<sup>5</sup>, Departmental POPIA Policy (2022) and the Standard Operation Procedure 2 of 2017: Processing of data requests.

## 6. Legislative Framework

- 6.1 The Post-School Education and Training Information Policy (PSETIP), (DHET, 2019)<sup>6</sup>, requires the Department to develop a data reporting system for PSET, and for information from such a system to be made available to the public, according to a publication and/or data dissemination standard.
- 6.2 Section 21 of the PSETIP also stipulates that the Department must ensure that the dissemination of data does not breach the appropriate rules of confidentiality as stipulated in Section 17 of the Statistics Act (1999)<sup>7</sup>.
- 6.3 The Promotion of Access to Information Act, (2000)<sup>8</sup> requires the Department to make information available to the public. At the same time, the Department has to ensure that confidential data is not disclosed to third parties.
- 6.4 The POPI Act, (2013)<sup>9</sup>, PSETIP (2019), and the POPIA Policy (2022) require the Department to ensure that confidential data acquired by the Department through its data collection systems are protected. The Act gives effect to the constitutional right to privacy, by safeguarding personal data when processed by the responsible party<sup>10</sup>.
- 6.5 According to Section 19 (1) of the POPI Act, the Department has the responsibility to ensure that the integrity and confidentiality of personal information in its possession is protected by taking appropriate, reasonable technical and organisational measures to prevent unlawful access to or processing of personal information.

---

<sup>5</sup> DHET (2021). Data Dissemination Standard. Government Gazette, No. 46366, 13 May 2022.

<sup>6</sup> DHET (2019). Post-School Education and Training Information Policy. Government Gazette No. 43073, 06 March 2020.

<sup>7</sup> Statistics South Africa, Statistics Act, 1999 (Act No.6 of 1999). *Government Gazette*, No. 29206, 15 September 2006.

<sup>8</sup> Republic of South Africa (2000). Promotion of Access to Information Act (Act 2 of 2000). *Government Gazette*, No. 20852, 3 February 2000.

<sup>9</sup> Republic of South Africa (2013). Protection of Personal Information Act (Act No. 4 of 2013). *Government Gazette*, No. 37067, 26 November 2013.

<sup>10</sup> Responsible party refers to data managers/officials/third parties who have access to confidential data.

- 6.6 In securing personal data, trust and confidence between the Department and individuals/entities/institutions providing data to the Department must be maintained.
- 6.7 The South African Statistical Quality Assessment Framework (SASQAF)<sup>11</sup> stipulates that there must be a law or policy that ensures that individual data are kept confidential and used only for statistical/administrative purposes.
- 6.8 The Data Confidentiality Standard is therefore informed by the POPI Act, the Promotion of Access to Information Act, SASQAF, the POPIA Policy and the PSETIP.

## 7. Lawful conditions

POPIA places a responsibility on the Department to promote the lawful processing of personal information and its service providers who act on behalf of the Department. POPIA consist of eight conditions which are adopted by the Department's POPIA Policy as principles guiding the Department to comply with the obligations created by the POPIA. The conditions are as follows:

<b>Accountability</b>	The Department is accountable and responsible for personal information in its possession at the Departmental level and shall comply with all the 8 POPIA conditions.  Branches are accountable and responsible for the personal information they process in their respective Chief Directorates, Directorates and Sub-Directorates and Project Offices. Each employee is responsible to comply with POPIA and POPIA Policy (2022) as they process personal information in their different areas of work.
<b>Data subject participation</b>	The Department shall establish mechanisms and processes to provide data subjects with the opportunity to request, correct, delete or destroy their personal information insofar as requests have been done in the prescribed manner and where possible and justifiable.
<b>Further processing limitation</b>	The further processing of any personal information must be compatible with the purpose for which it was initially collected.
<b>Information quality</b>	The Department shall take reasonable steps to ensure that the personal information it processes, and stores is complete, accurate, not misleading and kept up to date where necessary.
<b>Openness</b>	The Department must maintain the documentation of all processing operations under its responsibility. The purpose of this condition is to ensure transparency and fairness in the processing of personal information.

<sup>11</sup> Statistics South Africa, South African Statistical Quality Assessment Framework, 2010, 2<sup>nd</sup> edition.

	<p>The Department shall ensure that the data subject is aware of the reasons for which his/her personal information is processed. The Department shall inform data subjects of any breaches relating to the data subjects' personal information.</p>
<b>Processing limitation</b>	<p>The Department shall ensure that the processing of any personal information is done in accordance with the relevant legislation without infringing on the data subject's right to privacy.</p> <p>The Department shall ensure that personal information is only processed if the reasons given for the processing are adequate, legitimate, relevant and not excessive. Personal information shall be processed for the purpose it was collected for and not for a different purpose unless in accordance with exceptions in the Act.</p>
<b>Purpose specification</b>	<p>The Department shall only collect personal information for a specific purpose which is explicit and limit the processing to the specific purpose it was collected for. The Department must ensure, in collecting the information, that the data subject is aware of the purpose for which the information is being collected.</p>
<b>Security safeguards</b>	<p>The Department shall secure the integrity and confidentiality of personal information in its possession through the implementation of appropriate measures to prevent the loss, damage and unauthorised destruction of personal Information and unlawful access which leads to processing of personal information without the consent of the data subject.</p> <p>The Information Technology (IT) directorate will guide the Department in terms of what are the appropriate IT security technologies to ensure the safeguarding and protection of automated personal information and educate employees on protecting and securing automated processing of personal information.</p> <p>Physical Security and Asset Management will guide the Department in terms of appropriate security measures and facilities to ensure the safeguarding and protection of non-automated personal information.</p> <p>The Department shall also ensure that it has written agreements with all third parties processing personal information on its behalf. These agreements will need to outline the third party's measures to ensure the protection of personal information in their possession.</p> <p>The Department shall establish and implement processes or mechanisms to notify a data subject and the Information Regulator where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.</p>

## 8. Applicability

- 8.1 This standard applies to Departmental officials who in any manner collect, receive, record, organise, collate, store, update, alter or modify, retrieve, use, disseminate, merge, erase or destroy personal data and information contained in the MIS of the Department.
- 8.2 This standard applies to the Department (specifically to data managers) and entities to which the Department provides unit level record data in terms of statutory requirements for data sharing, or for auditing purposes, and also to service providers who might have access to unit level record data when developing and or maintaining systems for the Department.
- 8.3 All officials who have access to confidential data in the Department and handle data in any format and at any stage of the statistical production process as well as auditors who might require access to confidential data must sign the data declaration form, **Appendix 1**. Service providers/entities who might have access to confidential data when developing and/or maintaining information systems for the Department as well as those involved in undertaking data audits will also sign **Appendix 2** of the declaration form.
- 8.4 If any conflict arises between the provisions of the Data Confidentiality Standard and the Protection of Personal Information Act, 2013, the provisions of the latter must prevail.

## 9. Disseminated data

- 9.1 Disseminated data shall be presented in a way that an individual cannot be identified from the information as stipulated in the Data Dissemination Standard of the Department of Higher Education and Training (DHET, 2021)<sup>12</sup>.
- 9.2 All individuals who have access to confidential data in the Department shall only use the data in line with the approved purpose(s) for which the data provided was intended, and not disseminate it to a third party. Furthermore, they must ensure that the confidentiality of the data is always maintained.
- 9.3 Personal data may also be released during data audits in the Department. However, any person or representative of an organisation/entity/institution with access to that information will be expected to sign the declaration form.

---

<sup>12</sup> DHET (2021) Data Dissemination Standard. Government Gazette, No. 46366, 13 May 2022.

## 10. Conditions of handling data

- 10.1 Data should be protected from inappropriate access, use and disclosure by ensuring that personal laptops, unencrypted memory sticks and data stored on cell phones are password protected to prevent unauthorised and illegitimate access.
- 10.2 Workstations/offices must be locked if the user is leaving the computer unattended.
- 10.3 When completed questionnaires are being destroyed, they should be disposed of in a manner that does not compromise the confidentiality of their contents.
- 10.4 The Department through its Government Information Technology Office (GITO) will ensure that the networks are protected from unauthorised access and hacking.
- 10.5 Passwords for workstations must not be shared with anyone, including line managers and/or senior managers.
- 10.6 GITO and consultants must not remotely access computers without users' consent.

## 11. Sharing of confidential data with a third party

- 11.1 The Department may share personal identifiable data with third parties for the following purposes, and under the following conditions:
  - a) For auditing purposes;
  - b) In response to a legal requirement; and
  - c) For the development and or maintenance of databases and/or software programmes of the Department.
- 11.2 The information mentioned above will be shared if it is in line with the POPI Act (2013).
- 11.3 All third parties will be expected to sign confidentiality forms (**Appendix 2**).
- 11.4 Should a third party breach confidentiality, the Department will undertake steps set out in the signed confidentiality forms.

## 12. Breach of confidentiality

- 12.1 In the case where identifiable data is inadvertently released to a third party, the responsible party must make the recipient aware of the error and instruct them to delete the data immediately.
- 12.2 Disciplinary steps following internal Departmental policies will be instituted for a data manager or any individual who releases confidential data and or information to third parties.

- 12.3 A legal procedure must be instituted against any service provider who unlawfully uses the Department's confidential data outside of the agreed upon services they are appointed to provide.

### 13. Bibliography

1. Department of Higher Education and Training (2022) Protection of Personal Information Act Policy, 13 October 2022.
2. Department of Higher Education and Training (2019) Post-School Education and Training Information Policy, *Government Gazette*, No. 43073, 06 March 2020.
3. Department of Higher Education and Training (2021) Data Dissemination Standard, *Government Gazette*, No 46366, 13 May 2022.
4. OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.
5. Republic of South Africa (RSA) (2013) Protection of Personal Information Act, 2013 (Act No. 4 of 2013). *Government Gazette*, No. 37067, 26 November 2013.
6. Statistics Denmark, Data Confidentiality Policy at Statistics Denmark, 2015.
7. Statistics South Africa, Concepts and Definitions for Statistics South Africa, 2017
8. Statistics South Africa Standard, Data Confidentiality, 2012.
9. Statistics South Africa, South African Statistical Quality Assessment Framework, 2010, 2<sup>nd</sup> edition.
10. Statistics South Africa, Statistics Act, 1999 (Act No.6 of 1999). *Government Gazette*, No. 29206, 15 September 2006.
11. Thomson Reuters: Practical Law, Data Protection in South Africa: overview

[https://uk.practicallaw.thomsonreuters.com/Browse/Home/Practice/DataProtection?transitionType=Default&contextData=\(sc.Default\)&comp=pluk](https://uk.practicallaw.thomsonreuters.com/Browse/Home/Practice/DataProtection?transitionType=Default&contextData=(sc.Default)&comp=pluk). Accessed: 03 July 2023

**14. Appendix 1 –Confidentiality Declaration Form for Departmental staff**

I, (full name/s and surname) ..... declare that I will not release any identifiable data (except if it is a legal requirement), to any person not sworn to the preservation of confidentiality, through the completion of Confidentiality Declaration Form.

I also recognise that the Department has an obligation to uphold the rights of individuals as stipulated in the Protection of Personal Information Act, 2013 (Act No.4 of 2013), Post School Education and Training Information Policy, 2019 and Departmental POPIA Policy, 2022.

Therefore, in this regard:

I acknowledge that I understand and accept the following statements:

- I am familiar with the Departmental data policies.
- I will use data only for legitimate Departmental use for which I am explicitly authorised, and I know that it is against Departmental policy to peruse or use Departmental records including, but not limited to, confidential data and or information for my personal interest or advantage.
- I will report any security and privacy violations to the HETIS Officer which includes, but not limited to, hacking of computers and loss of laptop and external storage devices.
- I understand that violation of these statements may lead to reprimand, suspension, dismissal or other disciplinary action consistent with the general personnel policies of the Department.
- I will ensure that Departmental data pertaining to individuals in my possession is password protected.
- I understand that the use of confidential data for personal purposes is prohibited.

Any breach or suspected breach of data confidentiality shall be reported immediately to the Departmental HETIS Officer.

**SIGNATURE:** .....

**DATE:** .....

**BRANCH:** .....

**DIRECTORATE:** .....

**Instruction:** Please retain a copy of this form for your records, and return a completed form to Departmental HETIS Officer via email at [HETIS.Officer@dhet.gov.za](mailto:HETIS.Officer@dhet.gov.za)

**15. Appendix 2 – Confidentiality Declaration Form for external organisations and entities of the Department**

Confidential agreement

Between

Department of Higher Education and Training

(hereinafter referred to as “**the Department**”)

And

Name of the Organisation: .....

(hereinafter referred to as “**the Organisation**”)

**1. Background**

- 1.1 The Department processes collected data to produce a statistics report on the PSET which serves as an important tool for planning, allocation of budgetary resources, monitoring and reporting purposes to inform policy and decision making. The institutions and SETAs providing data to the Department therefore need to be assured that their data are kept confidential in line with the existing national policy and legislation that regulates matters concerning the confidentiality of individual data.
- 1.2 The Promotion of Access to Information Act, (2000)<sup>13</sup> requires the Department to make information available to the public. At the same time, the Department has a duty to ensure that confidential data and or information about a third party is not disclosed.
- 1.3 The Protection of Personal Information (POPI) Act, (2013)<sup>14</sup>, Post-School Education and Training Information Policy (PSETIP), (DHET, 2019) and the Departmental Protection of Personal Information Act (POPIA) Policy, (DHET, 2022) requires the Department to ensure that personal data and or information acquired by the Department through its data collection systems are protected. The Act gives effect to the constitutional right to privacy, by safeguarding personal data and or information when processed by the responsible party.

---

<sup>13</sup> Republic of South Africa (2000). Promotion of Access to Information Act (Act 2 of 2000). Government Gazette, No. 20852, 3 February 2000

<sup>14</sup> Republic of South Africa (2013). Protection of Personal Information Act (Act No. 4 of 2013). *Government Gazette*, No. 37067, 26 November 2013.

- 1.4 According to Section 19 (1) of the POPI Act, the Department has the responsibility to ensure that the integrity and confidentiality of personal data and or information in its possession is protected by taking appropriate, reasonable technical and organisational measures to prevent unlawful access to or processing of personal data and or information.
- 1.5 In securing personal data and or information, the Department must maintain trust and confidence between the Department and individuals/entities/institutions providing data to the Department.
- 1.6 Examples of personal information/confidential data includes, but are not limited to:
  - 1.6.1 Name, such as full name, maiden name, mother's maiden name, or alias;
  - 1.6.2 Personal identification numbers;
  - 1.6.3 Address information, such as physical address or email address;
  - 1.6.4 Biometrics of the person;
  - 1.6.5 Telephone or cell phone numbers; and
  - 1.6.6 Banking details.
- 1.7 It is for the above mentioned reasons that a confidential agreement must be entered into between the Department and the organisation/entity having access to confidential information of the Department, to ensure the protection of personal data and or information.

2. Confidential obligations

I (full name/s and surname)..... representative  
of ..... (the name of the organisation/entity) declare  
the following:

- 2.1 The organisation/entity will not release any confidential data to third parties.
- 2.2 Access to confidential data and or information will only be granted to authorised people in the organisation/entity, who will be made aware of the confidentiality clause the organisation/entity has with the Department.
- 2.3 The organisation/entity also recognises that the Department has an obligation to uphold the rights of individuals as stipulated in the POPI Act No.4 of 2013, Post School Education and Training Information Policy, 2019 and the Departmental POPIA Policy, 2022.

- 2.4 The organisation/entity will ensure that confidential data and or information they have in their possession is always protected, by password protecting all the software containing confidential data and or information.
- 2.5 Any security and privacy violations will be reported to the Information Officer<sup>15</sup> of the Department which include, but is not limited to, hacking of computers and loss of laptop and/or external storage devices.

**NAME OF THE ORGANISATION:**.....

**DATE:**.....

**SIGNATURE OF THE AUTHORISED REPRESENTATIVE**.....

**Instruction:** Please retain a copy of this form for your records, and return a completed form to Departmental HETIS Officer via email at [HETIS.Officer@dhet.gov.za](mailto:HETIS.Officer@dhet.gov.za)

---

<sup>15</sup>According to the POPI Act (2013), an "Information Officer" of, or in relation to a public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17