Data Protection Procedures – General Operations

October 2022

Table of Contents

PREAMBLE

These procedures have been created to assist staff of The UWI comply with the University Data Protection Policy (2020) and by extension the legislation in the local jurisdiction within which they operate.

These are general procedures and might not apply to every scenario or sub-entity of The UWI. Therefore, please recognise that the content is not comprehensive, is being refined, and will evolve over time.

Since these are general procedures, the expectation is that, as time progresses, individual sub-entities will create their own procedures, or customise these, to address their specific needs. Until that is done, these are the procedures that should be used guide how staff operate when processing personal data.

1.0 Introduction

The UWI's Data Protection Policy (2020) states that The UWI will:

1. comply with both the Data Protection legislation and policies in the countries in which The UWI operates, and global Data Protection best practices;
2. protect the privacy rights of all students and staff (including applicants), and alumni;
3. ensure that the Personal Data and/or Sensitive Personal in The UWI's possession are kept safe and secure;
4. support staff of The UWI in meeting their legal responsibilities;
5. mandate that third parties processing data on behalf of the University observe this Policy;
6. respect the Data Protection rights of individuals; and
7. provide awareness training and support for staff who process Personal Data and/or Sensitive Personal Data.

These procedures are linked to, and should be read in conjunction with, the **University Data Protection Policy (2020)** and provide step-by-step instructions to University personnel and those acting on behalf of the University as sub-contractors/contractors. Outlined in these procedures are the actions to be taken in order to ensure that the staff member (or contractor), acting on behalf of The UWI (Data Controller) or Data Processor (non-UWI entity), do not breach The UWI Data Protection Policy (2020).

In addition to its body, these procedures contain the following appendices to assist the reader better appreciate the content:

- **Appendix 1** – Elements of Personal Data and Sensitive Personal Data; a listing of the Personal Data and Sensitive Personal Data currently, or likely to be, managed by the University;

- **Appendix 2** - The University entities, both academic and non-academic, to which these procedures apply;
- **Appendix 3** - The Data Protection Acts and Authorities across the Caribbean (in the 17 contributing territories of The UWI);
- **Appendix 4** - a list of The UWI global centres;
- **Appendix 5** - Data Protection Authorities across the Anglophone Caribbean (in the countries where The UWI has a Global centre);
- **Appendix 6** - Record of Personal Data and/or Sensitive Personal Data Collected;
- **Appendix 7 -** Personal Data and Sensitive Personal Data Access list template;
- **Appendix 8 –** Forms; and
- **Appendix 9** - Personal Data Request Procedures; to be used by persons, external agents as well as internal staff, irrespective of their level within The UWI, when requesting Personal Data.

2.0 Scope

These procedures apply to all Personal Data and/or Sensitive Personal Data managed by all constituent parts of The UWI and its staff (full-time, part-time, or sub-contractor) in the course of their work with/for the University and irrespective of the format (electronic or hard-copy) in which these data are managed. These procedures also apply to archival holdings.

3.0 Definitions

Alumni	Any individual who holds a PhD, Master's, Bachelor's or Associate degree, Diploma and Certificate from The University of the West Indies or The University College of the West Indies. *(From the UWIAA Constitution)*
Contractor	A natural or legal person (i.e., a living individual or entity) who agrees to undertake work for the University based on the terms of a specific contract between them and the University. Contractors are not considered staff of the University and, unlike staff, are independent and may, depending on the terms of the contract between them and the University, undertake work for multiple entities simultaneously and also, independent of the University, be responsible to meet their tax and other statutory obligations.
Data Executive	The head of a University department in which Personal Data and/or Sensitive Personal Data are managed – collected, stored, processed, and/or maintained.
Data Controller	The University of the West Indies.
Data Custodian	The person managing the actual data.

Data Processor	An external entity which manages (creates, collects, stores, disseminates, or disposes of) data on behalf of The UWI.
Data Requestor	Any individual (staff, student, external entity) who makes a request for Personal Data and/or Sensitive Personal Data.
Enterprise Systems Support (ESS)	ICT staff who work in any section which supports the University's Enterprise Systems.
Personal Data	Information relating to a *living* individual, or to an individual who has been *deceased for less than thirty years*, who is, or can be identified, either from the data by itself or from the data in conjunction with other information, which is in, or is likely to come into the possession of the Data Controller (The UWI). *(ref. Data Protection Policy (2020))*
Sensitive Personal Data	Specific categories of Personal Data. These are defined as data relating to a person's racial origin, political opinions or religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence, and trade union membership. *(ref. Data Protection Policy (2020))*
Staff	Persons in the employment of the University engaged in one, or a combination, of the following: teaching; research; the application of a well-defined body of technical knowledge, practices and skills in support of the University' mission; the overall management of the University and/or that of its systems and/or component parts in support of the University's mission. *(Adapted from Statutes and Ordinances 2012 – Revised May 15, 2014)*
Student	A person who is registered as a student of the University during a current academic year for a first or higher degree, diploma, certificate or such other qualification or courses of the University as may be approved by the Senate as qualifying a person for the status of a student, but does not include a student of an affiliated institution who is registered for examinations to the degrees, diplomas, certificates and other academic awards of the University. *(ref. Statutes and Ordinances 2012 – Revised May 15, 2014)*

4.0 Rule of Thumb

As stated in The UWI Data Protection Policy (2020), Personal Data refers to information relating to a *living* individual, or to an individual who has been *deceased for less than thirty years*, who is, or can be identified, either from the data by itself or from the data in conjunction with other information, which is in, or is likely to come into the possession of the Data Controller (The UWI). Sensitive Personal Data refer to specific categories of Personal Data. These are defined as data relating to a person's racial

origin, political opinions or religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence, and trade union membership.

Always manage (collect, create, store, use, share, and dispose of) Personal Data and/or Sensitive Personal Data about other people as carefully as you would wish Personal Data and Sensitive Personal Data about yourself to be managed.

5.0 Managing Personal Data and/or Sensitive Personal Data as Records

Personal Data and/or Sensitive Personal Data, managed (collected, created, stored, used, shared, and disposed of) by staff (or sub-contractors) as a result of their engagement with The UWI, form part of University records. These are therefore subject to the University Records Management Policy and its accompanying procedures and guidelines.

5.1. **Always** consult the Campus Records Management Unit at your campus (or the Campus Records Management Unit associated with your Centre location) in respect of the retention and disposal/destruction of the Personal Data and/or Sensitive Personal Data in your custody.

6.0 Creating Personal Data and/or Sensitive Personal Data

*(Ref. **#'s 1, 2, and 8** of the Data Protection Governing Principles outlined in The UWI Data Protection Policy - p.7)*

According to the Data Protection Governing Principles outlined in The UWI Data Protection Policy (2020), processing must be:

- Fair (principle #1);
- Lawful (principle #2); and
- Justified (#6)

When creating Personal Data and/or Sensitive Personal Data:

6.1. Unless these are based in fact and can be defended as accurate if challenged, do not make adverse comments about a Data Subject (the individual to whom the Personal Data and/or Sensitive Personal Data relates). Also, comments should directly related to the Data Subject's association with the University. Always bear in mind that the Data Subject has a right to ask to see what is written about them.

7.0 Obtaining Personal Data and/or Sensitive Personal Data

*(Ref. **#'s: 1, 2, 3, 5, and 6** of the Data Protection Governing Principles outlined in The UWI Data Protection Policy - p.7)*

When obtaining/collecting Personal Data and/or Sensitive Personal Data (7.1 – 7.3):

7.1. Only collect Personal Data and/or Sensitive Personal Data that are required. Even if information might be useful in the future, do not collect information outside the scope of the immediate activity for which the information is to be used.

Notes:

- The Data Executive is the competent authority who determines the kinds of Personal Data and/or Sensitive Personal Data that ought to be collected by their respective section *(see **Appendix 1** – Elements of Personal Data and Sensitive Personal Data)*. The Personal Data and/or Sensitive Personal Data to be collected by a section should be documented, perhaps in department/section procedures, and provided to staff in the section.
- Do not record Personal Data unnecessarily,
    - Example: If a student reveals Personal Data to a non-clinical member of staff who then uses that information to refer the student to a relevant professional or professional department. Any Personal Data, such as notes, recorded should be destroyed immediately after the interaction between the student and the non-clinical staff member.

7.2. Always consider whether depersonalised data, i.e., data which cannot be used to identify individuals would achieve the same result as data with identification (name, id#, etc.) included. If depersonalised data can be used, do not use data with identifiers included.

7.3. Always be transparent and honest with the Data Subject (the person to whom the Personal Data and/or Sensitive Personal Data relate) when trying to acquire information:

a. Ensure that the identity of the Data Controller (The UWI) as well as the Data Custodian (your department/unit, etc.) appears on any instrument used to collect the information, or is stated in conversation or email.
b. Consider inserting a 'Fair Processing' statement in the instrument (or online screen) to be used for Personal Data collection.

> The <*department/unit*> at the <*campus*> of The University of the West Indies will use your personal information for <*purpose*> and related purposes. We will keep your personal information only for as long as required for this purpose unless you agree to let us add you to our mailing list, in which case your information will be retained after the <*purpose*> has ended.
>
> May we add you to our mailing list?
> **[TICK WHICH APPLIES: YES☐ NO☐]**
>
> If you wish to be removed from our mailing list at any time, please email <*email address*> or the University Data Protection Officer (dpo@uwi.edu).

Notes:

1. If what is being obtained is Sensitive Personal Data, what should be included is an opt-in, rather than an opt-out box on the instrument. With **Sensitive Personal Data**, consent cannot be inferred from a failure to respond. To be clear, consent cannot be assumed just because the Data Subject has not clearly refused.
2. If the Personal Data are being obtained during a telephone (or instant message) conversation, and there is an intention to use, or a likelihood of using, the Personal Data for a further purpose, the Data Subject must be informed and asked to provide written consent.
3. The evidence of written consent should be retained for as long as the Personal Data and/or Sensitive Personal Data are retained.

c. Record the staff member who obtained the Personal Data and/or Sensitive Personal Data, the date it was obtained (collected), where it is to be stored and who will have access to it. *(See **Appendix 6** – Record of Personal Data and/or Sensitive Personal Data Collected.)*
d. Provide a brief description of the purposes for which the Personal Data and/or Sensitive Personal Data, which are being obtained, will be used.
e. If you know or believe that the Personal Data and/or Sensitive Personal Data being obtained will be used for purposes other than that for which they are being obtained, say so and obtain the consent of the Data Subject before obtaining the information. Obtaining ***informed consent*** is imperative if Personal Data are to be used for purposes other than those for which they were originally collected.

7.4. If Personal Data and/or Sensitive Personal Data are obtained from a party outside the University, or even from one within the University, outside your department/unit, check whether the party has been authorised by the Data Subject to share it. **Keep a record of the answer.**

7.5. If Personal Data and/or Sensitive Personal Data are obtained from a party outside the University, or even from one within the University, outside your department/unit, check how accurate the party providing the Personal Data believes it to be. **Keep a record of the answer.**

7.6. If there is doubt about the accuracy of the Personal Data and/or Sensitive Personal Data obtained from a party outside the University or even from one within the University outside your department/unit, record this. **This might become important if you have to respond to a request from the University Data Protection Officer (dpo@uwi.edu) as a result of a complaint from the Data Subject or a request from the Data Protection Authority in the Data Subject's jurisdiction.**

If you do not have explicit consent and are unsure whether the collection of Personal Data and/or Sensitive Personal Data violates the University's Data Protection Policy **contact your supervisor/manager**, before you begin collection, who may then contact the **University Data Protection Officer (dpo@uwi.edu)** for clarification.

8.0 Using and Storing Personal Data and Sensitive Personal Data

Care must be taken when handling (using and storing) Personal Data and/or Sensitive Personal Data.

8.1. Personal Data and/or Sensitive Personal Data should be used only for the purposes for which they were collected or for compatible purposes in line with what was indicated to the Data Subject.

8.2. A case in point. Unless the Data Subject consents to this different use, data collected for research purposes should not be used for marketing purposes.

8.3. Staff must be especially careful when handling Sensitive Personal Data. The following are important considerations to note:

a. Explicit/written consent must be provided before handling; **or**

b. Handling should be essential for the job tasks to be undertaken (Data Executive to determine who/roles has access and the kind of access – **(***See* ***Appendix 7*** *- Personal Data and Sensitive Personal Data Access list template*)); **or**

c. One of the following justifications should apply

i. the information is already in the public domain;

ii. handling is lawfully required for employment purposes;

iii. handling is required to protect the interests of the Data Subject or another individual and the option of obtaining consent is unavailable or impractical;

iv. handling is required for legal proceedings, to obtain legal advice, or to establish or defend legal rights.

Note: Staff should contact the University Data Protection Officer (dpo@uwi.edu), through their supervisor/manager, if they are unable to determine if the justifications can be used.

Transferring Personal Data and/or Sensitive Personal Data to devices (PCs, etc.)

8.4. Personal Data and/or Sensitive Personal Data **should not** be transferred (copied or downloaded) from any of the University's enterprise resource planning (ERP) systems, e.g. PeopleSoft, Banner, TMA, etc., unless it is **absolutely necessary** to do so. Absolute necessity means that the information cannot be used from within the ERP to do the work of the University.

Note: The staff member should not, on their own, determine when it is necessary to transfer Personal and/or Sensitive Personal Data. Instead, staff should consult the Data Executive, or immediate supervisor, for their unit when determining **absolute necessity**.

a. This stipulation should be observed regardless of the owner of the device in question and applies equally to University-owned devices, assigned to the staff member or available to the staff member for use, and those not owned by the University.

b. This stipulation should be observed whether the staff member is operating from University property or outside.

c. This stipulation should be observed whether the staff member connects to University ERPs via the University's (at whatever campus or Centre location) Virtual Local Area Network (VLAN).

8.5. Staff should contact the relevant Campus IT Services unit, whether directly or through their supervisor/manager, to ensure that they are able to access computing services, including ERPs (e.g. Banner and PeopleSoft). Such access should be based on their job role and should allow the staff member to be able to do their assigned duties without hindrance.

8.6. Where the circumstances warrant the transfer of Personal Data and/or Sensitive Personal Data to a staff member's device (PC, etc.), whether or not that device is owned by the University or assigned to the staff member:

a. The staff member must ensure that any Personal Data and/or Sensitive Personal Data managed by the University is secure. While the University, as the Data Controller, is ultimately responsible for the protection of the Personal Data and/or Sensitive Personal Data under its management, if the security of the staff member's device is compromised (hacked, stolen, etc.), the staff member will be held accountable for the Data Protection breach. *(Seek guidance from your IT Services section for assistance with securing your device.).*

b. The staff member must ensure that any Personal Data and/or Sensitive Personal Data managed by the University is not shared with unauthorised persons. *(See **Appendix 7** - Personal Data and Sensitive Personal Data Access list template.*)

c. Any and all Personal Data and/or Sensitive Personal Data transferred to a staff member's device should be deleted from that device as soon as the data have been used for the purpose for which they were transferred in the first place.

E.g. Personal Data and/or Sensitive Personal Data transferred to a staff member's device in order to compile a report should be deleted once the report has been compiled. The Personal Data and/or Sensitive Personal Data in the compiled report should, where possible, be anonymised (identification fields deleted) or pseudonymised (identifiers with replaced pseudonyms) to minimise the possibility of identifying the Data Subject if the device is compromised.

Securing Personal Data and/or Sensitive Personal Data

8.7. The username and password, together referred to as credentials, provided to you for accessing University systems allow you access to Personal Data and/or Sensitive Personal Data. Anyone, including colleagues in your department/unit, with access to your credentials might be able to access information which you alone should have access to. Remember, Data Protection is about disclosure to unauthorised persons, therefore, if someone else uses your credentials to access Personal Data and/or Sensitive Personal Data, this is a Data Protection breach. To prevent this:

a. Ensure that your credentials are kept secure at all times; and

b. If you have even the slightest doubt whether your credentials have been compromised, treat this as a possible Data Protection breach. Immediately request a password change from IT Services. Report it to your supervisor.

8.8. Do not leave hard/paper copies of Personal Data and/or Sensitive Personal Data in a location where anyone but you can access them (look at, pick up, destroy, etc.).

8.9. Store hard/paper copies of Personal Data and/or Sensitive Personal Data in a secure, locked location accessible only by persons authorised to handle this information.

8.10. If Personal Data and/or Sensitive Personal Data are held on, or accessible from, a device assigned to, or owned by, you, **never** leave it unattended without locking the screen.

8.11. If Personal Data and/or Sensitive Personal Data are held on, or accessible from, a device assigned to, or owned by, you, and someone who is not authorised to see these data are in a place where they can view the data, change location, lock the screen or indicate to them that they cannot remain at their present location. If the situation is one where you, or the person, are/is unable to change location, **report the matter to your supervisor** and indicate the potential for a Data Protection breach.

a. Personal Data and/or Sensitive Personal Data transmitted, whether within or outside The UWI, must be done with the appropriate level of security. Ensure the following:
b. If the Personal Data and/or Sensitive Personal Data are being transmitted in hard-copy, whether internally or externally, ensure that this is done in a sealed envelope and alert the recipient when it has been dispatched.
c. If possible, electronic communication should be encrypted.
d. If possible, electronic files should be password protected. If the recipient needs to be sent the password, it should be transmitted in a separate communication and, if possible, using a communication mode different from the one used to transmit the initial file.
e. If Personal Data and/or Sensitive Personal Data are being transmitted electronically (e.g. via email), whether internally or externally, the email should be labelled 'CONFIDENTIAL'.

Communication via Telephone

f. Disclosure of Personal Data and/or Sensitive Personal Data oftentimes takes place over the telephone. Take the following precautions:
g. Always check the identity of the person requesting, via telephone, Personal Data and/or Sensitive Personal Data. This applies to co-workers or those purporting to represent persons of high authority within or outside The UWI.
h. Even if disclosure is agreed to via telephone, this should be accompanied by a Personal Data Request Form (See Appendix 8 – Personal Data Request Procedures)

9.0 Protecting Personal Data and/or Sensitive Personal Data in mail and email

*(Ref. **#4** of the Data Protection Governing Principles outlined in The UWI Data Protection Policy - p.7)*

Always ensure the following:

9.1. **When sending the same email message to more than one recipient.**
Unless you **intend to share** with all recipients the email addresses of those to whom the message is being sent and are **in no doubt** that recipients' email addresses (which is Personal Data) are already **known to all other recipients** and sharing email addresses is of no consequence (e.g. when recipients are in the same unit/department, part of the same internal group, etc.), **always** use 'bcc' (blind carbon copy) instead of 'cc' (carbon copy) when adding the email addresses of those to whom the message should be sent.

Remember: The Data Subject **must** give written consent for their Personal Data (even email address) to be shared.

9.2. Personal Data should be removed from envelopes which are re-used. Removal includes redacting or covering the information to make it illegible. Remember, someone's name and address (home and/or work) are considered Personal Data.

9.3. Incoming and outgoing traditional (snail) mail and emails containing Personal Data and/or Sensitive Personal Data should either **filed** or **deleted** once the action to which they relate has been completed. If these mail and email can be filed or deleted before the action to which they relate has been completed, without prejudicing the action, this should be done.

9.4. Email containing Personal Data and/or Sensitive Personal Data which remain in a member of staff's (or contractor's) inbox awaiting the conclusion of a particular action to which these relate, should be reviewed at regular intervals, protected, and placed in specific email folders in order for easy deletion.

9.5. Personal email received at your UWI email account should be placed in email folders separate from the Personal Data and/or Sensitive Personal Data received as a part of your work activities. These emails should also be scrutinised and routinely deleted to ensure your privacy and the privacy of anyone whose information might be contained in those personal, non-work-related, emails.

10.0 Non-UWI parties handling the Personal Data and/or Sensitive Personal Data of UWI Data Subjects

For all Personal Data and/or Sensitive Personal Data to be managed by Non-UWI parties, the following are to be considered:

10.1. A **Non-UWI party** refers to a natural or legal person, public authority, agency or body other than the Data Subject and The UWI who is authorised, by The UWI, to manage (collect,

create, store, use, share, and dispose of), on behalf of The UWI, the Personal Data and/or Sensitive Personal Data of individuals.

10.2. **Written contracts** between The UWI and non-UWI external entities (also known as Processors of Personal Data and/or Sensitive Personal Data) should exist to ensure a common understanding of their mutual obligations, responsibilities and liabilities.

10.3. Whenever The UWI (whichever UWI entity) uses a non-UWI entity to manage (collect, create, store, use, share, and dispose of) Personal Data and/or Sensitive Personal Data on its behalf, **a written contract should be in place between The UWI and the external entity (Data Processor) before Personal Data and/or Sensitive Personal Data are shared with the external entity, and/or before the external entity collects Personal Data and/or Sensitive Personal Data on behalf of The UWI**.

10.4. Similarly, if the external entity (i.e. the Processor) uses another organisation (i.e. a Sub-processor) to assist with managing Personal Data and/or Sensitive Personal Data for The UWI, **the Processor should have a written contract in place with that Sub-processor before Personal Data and/or Sensitive Personal Data are shared with the Sub-processor, and/or before the Sub-processor collects Personal Data and/or Sensitive Personal Data** on behalf of Processor which is itself acting on behalf of The UWI.

10.5. **What needs to be included in the contract?**

Contracts should include:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and/or Sensitive Personal Data and categories of data subject (e.g. student, staff, alumni, donors); and
- The UWI's obligations and rights.

Contracts should also include specific terms or clauses regarding:

- processing only on The UWI's documented instructions;
- maintaining confidentiality;
- appropriate security measures;
- using Sub-processors;
- the rights of data subjects;
- audits and inspections; and
- end-of-contract provisions.

11.0 Data Breach Management

A data breach might take place due to any number of reasons. Whatever the reason, the data breach must be reported without delay by staff to the authorised officer (Data Executive or immediate

supervisor), who in turn will immediately notify the Data Protection Officer. If the authorised officer is the person who commits the breach, he or she should immediately report this to the Data Protection Officer. *(To make the report, use the "Possible Personal Data and/or Sensitive Personal Data Breach – Incident Report" in Appendix 8.)*

This applies to all who handle Personal Data and/or Sensitive Personal Data on behalf of The UWI. The persons include:

- Any person who has access to University-controlled (acquisitioned, processed, stored, or outputted) Personal Data and/or Sensitive Personal Data
    - Staff employed to The UWI;
    - Students (including exchange students);
    - Visitors (including visiting scholars, researchers and exchange staff);
    - Data Processors
        - Contractors, part-time staff, and affiliated individuals (who have access to The UWI systems but are not employed to the institution);
        - Persons employed to contractors who process University data

This applies to all University-controlled (acquisitioned, processed, stored, or outputted) Personal Data and/or Sensitive Personal Data, such as:

- **[Location]** All Personal Data and/or Sensitive Personal Data whether managed using the IT systems owned by The UWI, any other IT systems, including email, Cloud-based platforms, or IT system of a company or individual to which/whom Personal Data and/or Sensitive Personal Data management has been sub-contracted.
- **[Format]** All Personal Data and/or Sensitive Personal Data managed in any format, digital and non-digital;
- **[Hardware/Device]** All Personal Data and/or Sensitive Personal Data whether managed on a University-owned device or on another device not owned by the University;
- **[Management]** All Personal Data and/or Sensitive Personal Data whether managed using The UWI's central (including by the Technology Services division at a campus) IT systems or distributed IT systems of a Faculty/School, Division, Institute, Centre, Department or Unit.

11.1 Determining whether a Personal Data and/or Sensitive Data Breach occurred

Determining whether an incident rises to the level of a Personal Data and/or Sensitive Personal Data breach should be done on a case-by-case basis. Not all incidents involving Personal Data and/or Sensitive Personal Data are data breaches. Although it is not possible to provide a comprehensive list of Personal Data and/or Sensitive Personal Data breaches, some of the more common examples of Personal Data and/or Sensitive Personal Data breaches are listed below.

- **Accidental Destruction**
    - Inadvertently deleting an electronic file or destroying a physical one. **Note:** If there exists a full and up-to-date back-up of the Personal Data and/or Sensitive Personal Data which were deleted, this might not constitute a Personal Data breach.
- **Loss**
    - Equipment (laptop, smartphone, tablet, external hard-drive, flash/thumb drive) on which Personal Data and/or Sensitive Personal Data are stored, or hard-copy records, are misplaced – even temporarily ***(see 4.1.1)***.
    - Equipment on which Personal Data and/or Sensitive Personal Data are stored fails/crashes causing data to be unrecoverable.
    - Breaches of physical security (e.g. break-ins to filing cabinet or other storage medium; break-ins to rooms/spaces) in areas where Personal Data and/or Sensitive Personal Data are housed. [This scenario might also lead to Unauthorised Access.]
- **Alteration**
    - Changing an entire, or parts of a, data record in error.
    - Deleting an entire, or parts of a, data record in error.

- **Unauthorised Disclosure or Unauthorised Access**
    - **Human error** – inadvertently disclosing Personal Data and/or Sensitive Personal Data to an individual whom it was thought had the requisite authorization to view/process this data.
    - **Accidental disclosure**
        - Inadvertently disclosing the wrong type of Personal Data and/or Sensitive Personal Data to an individual who has the requisite authorization to view/process this data. E.g. more data than what they are authorized to view/processed is disclosed to the individual in fulfilling a legitimate Personal Data request.
        - Leaving confidential information in accessible areas or leaving a device which is logged-in to an information system, application, data repository (including local storage), or electronic mail unattended.

    - **Inappropriate/insufficient IT controls and/or precautions**
        - Allowing transfer of information to external or unauthorised IT systems. E.g. uploading Personal Data and/or Sensitive Personal Data to an unauthorised website, domain or third-party service.
        - Allowing access to Personal Data and/or Sensitive Personal Data using insecure credentials.
        - Malware attacks or information security intrusions on IT infrastructure allowing unauthorised users access to Personal Data and/or Sensitive Personal Data.

Note: If Personal Data and/or Sensitive Personal Data are securely encrypted or anonymised, this might not constitute a Personal Data breach.

- Not collecting logs and other sources of access, authentication and authorisation activity – normally used for monitoring, reviewing, and evaluating suspicious activity.

11.2 Management of a Data Breach

There are three steps to managing a Data breach:

1. Collection of Incident Details;
2. Notification of Data Breach and Risk Assessment;
3. Evaluation and Response.

11.2.1 Incident Details

Details of the incident should be recorded accurately by the authorized officer including:

i. Description of the incident;
ii. Date and time of the incident;
iii. Date and time the incident was detected;
iv. Who reported the incident and to whom it was reported;
v. The type of Data involved and its sensitivity;
vi. The number of individuals affected by the breach;
vii. Whether the Data were encrypted?
viii. Details of any Information Technology (IT) systems involved;
ix. Corroborating material(s).

11.2.2 Notification of Data Breach & Risk Assessment

Internal Notification

i. Having become aware of a suspected, potential or actual Personal Data and/or Sensitive Personal Data breach the staff member or contractor shall immediately report the **incident** to the head of their area (Unit/Department/School/Faculty/Division) or, in the case of contractors, University contact.

ii. The head of their area (Unit/Department/School/Faculty/Division) or, in the case of contractors, University contact, shall, upon receipt of the report, then make a preliminary **incident** report to the Data Protection Officer (dpo@uwi.edu).
The incident report should address the following questions:
    1. What type of data are involved?
    2. How sensitive are the data involved?
    3. How many individuals' Personal Data and/or Sensitive Personal Data are affected by the breach?
    4. Were there protections (e.g. encryption) in place?

5. What are the potential adverse consequences for individuals and how serious or substantial are they likely to be?
6. How likely is it that adverse consequences will materialize?

iii. After reporting the incident, the head of area (Unit/Department/School/Faculty/Division) or, in the case of contractors, University contact, shall, complete the **Possible Personal Data Breach - Incident Report** *(See – "Personal Data Breach Incident Report" in Appendix 8)* within 24 hours or as soon as they are able to do so.

iv. The Data Protection Officer shall then determine how best to address the breach.

11.2.3 Evaluation and Response

Subsequent to any Personal Data and/or Sensitive Personal Data breach, a thorough review of the incident will be made by the Data Protection Officer. The purpose of this review will be to:

i. Ensure that the steps taken during the incident were appropriate;
ii. Describe and record the measures taken to prevent a repetition of the incident;
iii. Identify areas in need of improvement;
iv. Document any recommended changes to the Policy and/or Procedures.

12.0 Awareness Training & Support for Staff who process Personal Data

The UWI aims to support staff members who process Personal Data and/or Sensitive Personal Data, through Data Protection Awareness Training and Data Protection support mechanisms.

12.1 Data Protection Awareness Training

Data Protection Awareness Training will take place during the orientation of new staff, and at various intervals throughout an employee's professional career at The UWI. Training sessions will be conducted at least once each academic year.

12.2 Data Protection Support

Data Protection Support is provided by the individual(s) performing the role of Data Protection Officer(s).

13.0 Compliance Audits (Risk Management)

13.1 Internal Compliance Audit

The main purpose of an Internal Compliance Audit is to determine whether The UWI is operating in accordance with the relevant Data Protection legislation and policies and to identify possible

contraventions of the legislation and policies. Compliance audits will be the purview of The University Auditor and will form part of the University's Compliance Framework.

i. Annual Internal Compliance Audits will be undertaken by members of one or more of the following: the Data Protection Working Group; the Data Protection Officer; the University Management Audit Department; any other authorized unit. The purpose of these audits is to identify existing and potential risks.
ii. Internal Compliance Audits will review both manual and electronic Data Procedures and compliance.
iii. In order to ensure that the requirements of the Data Protection legislation and policies are observed, immediate remedial action may be prescribed by the auditor / audit team.
iv. Managers/ Staff shall cooperate fully with the auditor/ audit team in completing Internal Compliance Audit questionnaires and site visits.
v. Audit results will be recorded.

Appendices

Appendix 1 – Elements of Personal Data and Sensitive Personal Data

Personal Data and Sensitive Personal Data include, among other things:

(**Note:** Some elements apply to both staff (including contractors and temporary staff) and students, others apply to only either staff only (†) or students only (*).)

Personal Data	Sensitive Personal Data

• **Biographic Data**
  ○ Date of birth
  ○ City of birth
  ○ Birth certificate
  ○ Age
  ○ Weight
  ○ Height
  ○ Gender
  ○ Eye colour
  ○ Hair colour
• **Contact Details**
  ○ Address
  ▪ Work address (†)
  ▪ Current home address
  ▪ Previous addresses
  ○ Email
  ▪ Personal email address
  ▪ UWI provided email address
  ○ Length of time at current residence
  ○ Telephone number
  ▪ Home phone
  ▪ Mobile/Cell number
  ▪ Work phone
• **Education Data**
  ○ Certificates
  ○ Education history
  ○ Schools attended
  ○ Transcripts
• **Identification Data**
  ○ Driver's license / state ID
  ○ Immigration information (student visa) *
  ○ Nationality
	• **Biometric data**
	  ○ Biometric identifiers
	  ▪ Facial geometry
	  ▪ Fingerprint
	  ▪ Hand shape
	  ▪ Retina scan
	  ▪ Vein Pattern
	  ▪ Voice signature
	  ○ Handwriting
	  ○ Signature
	  ○ Writing sample (electronic)
	• Disabilities
	• Family health history
	• Financial Data (Sensitive)
	  ○ Bankruptcies
	  ○ Liens
	  ○ Pardons
	  ○ Tax returns
	• Genetic information
	• Health Data
	  ○ Health insurance records
	  ○ Medical records
	  ○ Medical card number
	  ○ Prescriptions
	• **Justice System related Data**
	  ○ Alleged criminal activity
	  ○ Arrest records
	  ○ Criminal offenses and convictions
	  ○ Judgements
	• Physical or mental disability
	• **Political Data**
	  ○ Voter registration records
	  ○ Political party affiliations & opinions

Personal Data	Sensitive Personal Data
○ National ID ○ Passport ▪ Passport information ○ Social security / social insurance number / Taxpayer Registration Number ○ Student ID • **Name** ○ First name ○ Last name ○ Maiden name ○ Other names used ○ Username • **Occupation Data** (†) ○ Occupation ○ Current employer ○ Employment history ○ Performance evaluations ○ Reference interviews ○ HR issues & disciplinary actions ○ Marital status ○ Spouse's name ○ Parents' names ○ Children's names • **Multimedia Data** ○ Face photographs ○ Other identifying photographs ○ Photo location data ○ Video footage ○ Voice recording • **Financial Data** ○ Bank account ○ Credit card number ○ Credit report ○ Current income ○ Debit card number ○ Homeowner status ○ Home value ○ Income history ○ Investment records ○ Life insurance records ○ Loan records ○ Other financial statements ○ PIN number ○ Property records	• Racial & ethnic origin ○ Ethnicity • Religion & philosophical beliefs • Sexual orientation • Sexual partners • Trade union membership • Veteran status

Personal Data	Sensitive Personal Data

• **General Personal Data**
  o Activity on a UWI website
  o Car insurance records
  o Contacts list
  o Email records
  o Event attendance (UWI)
  o Friends' names
  o Likes & ratings
  o Media preferences
  o Messages on the site (UWI)
  o Number of people in household
  o Pets & animals
  o Professional license records
  o Recreational license records
  o Siblings' names
  o Search history on the site (UWI)
  o Topics of interest
  o Website
  o Vehicle registration records
• **IT Data (including metadata)**
  o Browser
  o Cloud storage files
  o Cookies
  ▪ Session
  ▪ HTTP-only
  ▪ Authentication
  o Current location (physical)
  o Device ID / MAC address
  o IP address
  o ISP
  o Language preference
  o Location history (physical)
  o Operating system
  o Password
  o Security question & answer
  o Shopping & purchase history (on the site)Social media accounts
  o Social media posts & history
  o Third-party login	

Appendix 2 – University entities to which these procedures apply

These procedures apply to both academic and non-academic entities across the University

A2.1.1 Academic

Campus	Faculty/School/Specialised Research Units and Centres
Cave Hill	• Culture, Creative and Performing Arts • Humanities and Education • Law • Medical Sciences • Science and Technology • Social Sciences • Sport
Five Islands	• Business and Management • Health and Behavioural Sciences • Humanities and Education • Science, Computing and Artificial Intelligence
Mona	• Engineering • Humanities and Education • Law • Medical Sciences • Science and Technology • Social Sciences • Sport
Open Campus	• Continuing and Professional Education • Postgraduate • Undergraduate
St Augustine	• Engineering • Food and Agriculture • Humanities and Education • Law • Medical Sciences • Science and Technology • Social Sciences • Sport
Vice Chancellery	• Caribbean Institute for Health Research • Centre for Reparation Research (CRR) • Centre for the Environment • Diplomatic Academy of the Caribbean • Disaster Risk Reduction Centre • Global Institute for Climate Smart and Resilient Development • Institute of Criminal Justice and Security • Institute for Gender and Development Studies

	• Institute for Sustainable Development • Institute of International Relations • Latin American Caribbean Culture • Sir Arthur Lewis for Social and Economic Research

A2.1.2 Non-academic

Campus	Entity	Sub-entity
Cave Hill	Academy of Sport	
	Senior Administration	• Office of the Campus Principal • Office of the Deputy Principal • Office of the Campus Registrar • Office of the Campus Bursar • Senior Administration and Faculty Deans
	Administrative Offices	• Alumni Relations • Bursary • Business Development Office • Campus IT Services • Campus Registrar • Centre for Excellence in Teaching and Learning • Centre for Professional Development and Lifelong Learning • Credit Union • Graduate Studies and Research • Hall Accommodation • Human Resources Section • International Office • Office of Planning & Infrastructural Service • Office of Marketing and Communications • Office of Research • Office of Student Services • Sidney Martin Library (formerly Main Library) • Student Enrolment and Retention Unit (SERU)
	Archives and Records Management	• Campus Records Centre • Office Management • Registry Records Services
	Campus Services	• Bookshop

Campus	Entity	Sub-entity
Cave Hill		• Bus Shuttle Service • Campus Security • Counselling and Psychological Services • Information Technology Service Desk • Student Guild • Student Health Services
	Student Affairs (Undergraduate)	• Admissions • Examinations • Examinations – Record Unit
	Libraries	• Audine Wilkinson Library • CLR James Cricket Research Centre Library • Elizabeth Watson AV Unit • Faculty of Medical Sciences Library • Law Library • Sidney Martin Library
Five Islands	Office of the Campus Principal	• Human Resources • Information Technology • Marketing • Office of Projects and Planning
	Office of the Director of Academic Affairs Enrolment Management Unit	• Admissions • Exams • Recruitment • Registration • Retention
Mona	Administrative Support Units	
	Health Centre	
	Registry	• Campus Records Management • Examinations Section • Human Resource Management Division • Marketing and Communications Office • Office of Admissions • Office of Graduate Studies and Research • International Students Office • Registry Information Systems • The Secretariat

Campus	Entity	Sub-entity
	Research and Education	• Centre for Excellence in Teaching and Learning • Office of Graduate Studies and Research • Office of Planning and Institutional Research • Office of Research and Innovation
	Other Services	• Campus Security • Security Directory • Estate Management Department (Maintenance Services) • Mona Information Technology Services • MONATS (Mona Non-Academic & Technical Staff) • University Press • UWI Development and Endowment Fund • WIGUT (West Indies Group of University Teachers)
	Student Services	• Bookshop • Bursary • Office of Student Financing (OSF) • Office of Student Services and Development • Placement and Career Services • Sports Development
Open Campus	• Academic Programming and Delivery • Accreditation • Business Development Unit • Computing and Technical Services • Continuing and Professional Education Unit • Consortium for Social Development and Research	

Campus	Entity	Sub-entity
Open Campus	• Graduate Studies & Research • Guild of Students • Human Resource Department • Marketing & Communication • Open Campus Country Sites • Open Campus Libraries • Quality Assurance Unit • Registry • Research Ethics Committee • Virtual International Students Office	
St. Augustine	• Admissions Section • Campus Bursary • Campus IT Services • Campus Office of Planning & Institutional Research • Campus Projects Office • Centre for Excellence in Teaching & Learning (CETL) • Development • Student Life And Development Department • Division of Facilities Management • Division of Student Services and • Estate Police • Examinations Section • Health Services Unit • Human Resources • Institutional Effectiveness Unit	

Campus	Entity	Sub-entity
St. Augustine	• International Office • The Alma Jordan Library • Marketing and Communications Office • Multimedia Production Centre • Occupational Health, Safety and the Environment Unit • Office of Graduate Studies and Research • Office of Research Development and Knowledge Transfer • Sports and Physical Education Centre	
	Campus Services	• Bookshop • Campus Security • Computer Sales • Sports & Physical Education Centre
	Student Affairs	• Academic Advising • Admissions - Postgraduate • Admissions - Undergraduate • Alumni Association • Awards & Scholarships • Career Guidance • Counselling & Psychological Services • Deputy Principal Office • Division of Student Services and Development • Off Campus Accommodation • On Campus Accommodation • Services for International Students • Study Abroad

Campus	Entity	Sub-entity
	Student Financial Administration	• Financial Information • Residence Fees • Scholarships & Bursaries • Tuition & Fees - Postgrad (PDF) • Tuition & Fees - Undergrad
Vice Chancellery	• Office of the Board for Undergraduate Studies • Graduate Studies and Research • Office of Administration • Office of Finance • Office of Global Affairs (OGA) • Office of Online Learning (OOL) • University Office of Planning • University Office of Global Partnerships and Sustainable Futures • Office of the University Chief Information Officer • The Caribbean Quarterly • The Legal Unit • The Quality Assurance Unit • The University Archives	

Appendix 3 – The Data Protection Legislation and Authorities across the Caribbean (in the 17 contributing territories of The UWI)

Country	Legislation
Antigua and Barbuda	Data Protection Act (2013)
Bahamas	Data Protection Act (2003)
Barbados	Data Protection Act (2019)
Bermuda	Personal Information Protection Act (2016)
Cayman Islands	Data Protection Act (2017)
Jamaica	Data Protection Act (2020) – **Not yet in full effect**
St. Kitts and Nevis	Data Protection Act (2018)
Saint Lucia	Data Protection Act (2011)
Trinidad and Tobago	Data Protection Act (2011) – **Partially in force**
St. Vincent and the Grenadines	Privacy Act (2003)

Caribbean Countries with Data Protection Legislation and Data Protection Authorities

Country	Data Protection Authorities
Antigua and Barbuda	Mrs. Joycelyn Palmer, Information Commissioner **Telephone:** (268) 562-7163
Bahamas	Mr Michael Wright Data Protection Commissioner Poinciana House, North Building, First Floor 31A East Bay Street, P.O. Box N-3017 Nassau, The Bahamas **Tel.:** 242-604-1000 **Cell.:** 242-376-7500 **Email:** dataprotection@bahamas.gov.bs
Barbados	Ms. Lisa Greaves, Data Protection Commissioner **Email:** lisa.greaves@barbados.gov.bb. **Telephone:** (246)-536-1212 (Direct); (246) 535-1200
Bermuda	Mr. Alexander White, Privacy Commissioner Office of the Privacy Commissioner for Bermuda **Email:** PrivCom@privacy.bm **Telephone:** (441) 543-7748
Cayman Islands	Ms. Sandy Hermiston, Ombudsman **Email:** info@ombudsman.ky **Telephone:** (345) 946-6283
Jamaica	Ms Celia Barclay Information Commissioner **Telephone:** (876) 920-4390
St. Kitts and Nevis	Office not yet set up
Saint Lucia	Office not yet set up

Trinidad and Tobago	Office not yet set up
St. Vincent and the Grenadines	Office not yet set up

Appendix 4 – List of The UWI Global Centres

(In alphabetical order)

Partnership/Global Centre	Country
Canada-Caribbean Institute (CCI)	Canada
CARIFORUM-EU Centre (CEC)	Italy
Glasgow-Caribbean Centre for Development Research (GCCDR)	Scotland
Joint UH-UWI Centre for the Sustainable Development of the Caribbean (JCSDC)	Cuba
Strategic Alliance for Hemispheric Development (UWIUNIANDES SAHD)	Columbia
SUNY-UWI Centre for Leadership and Sustainable Development	USA
UNILAG-UWI Institute of African and Diaspora Studies	Nigeria
UWI/Coventry Institute for Industry-Academic Partnership (Education and Research)	England
UWI-China Institute of Information Technology (UWI/CIIT)	China
UWI-University of Johannesburg Institute for Global African Affairs	South Africa

Appendix 5 – Data Protection Legislation in countries with UWI Global Centres

Country	Legislation
Canada	The Personal Information Protection and Electronic Documents Act (PIPEDA)(revised May 2019)
China	Personal Information Protection Law (PIPL) (2021) – took effect November 1, 2021
Columbia	– Articles 15 and 20 – Columbian Constitution (the right to privacy and the right to data rectification) – Statutory Law 1266 (2008) (Law 1266) (basic data processing principles, data subject rights, data controller obligations and specific rules for financial data)
Cuba	No legislation
England	Data Protection Act (2018)
Italy	General Data Protection Regulation (Regulation (EU) 2016/679 'GDPR')
Nigeria	Nigeria Data Protection Regulation (2019)
Scotland	General Data Protection Regulation (Regulation (EU) 2016/679 'GDPR') and Data Protection Act (2018)
South Africa	The Protection of Personal Information Act, 2013 (POPIA) (Act 4 of 2013) – took effect on July 1, 2020 (1 year grace period up to June 2021)
USA	No single principal Data Protection Legislation in the US. Most applicable to us (SUNY-UWI collab) the New York Privacy Act. **Not yet passed.**

Data Protection Legislation and Authorities in Countries with UWI Global Centres

Country	Data Protection Authorities
Canada	Daniel Therrien Privacy Commissioner of Canada Office of the Privacy Commissioner of Canada 30 Victoria Street Gatineau, Quebec K1A 1HE Email: genaral@oid-ci.gc.ca
China	**None yet**
Columbia	Andrés Barreto Superintendent of Industry and Commerce (SIC) Ministry of Commerce, Industry and Tourism Website: www.sic.gov.co
Cuba	**None**
England	Elizabeth Denham, Information Commissioner Information Commissioner's Office (ICO) Ico.org.uk
Italy	Italian Data Protection Authority is based in Rome.

	Piazza Venezia 11 - 00187 Roma (Italy) Phone: +39 06.696771 Email: protocollo@gdpd.it
Nigeria	NITDA HQ No. 28, Port Harcourt Crescent, Off Gimbiya Street, P.M.B 564, Area 11, Garki, Abuja, Nigeria. Email: info@nitda.gov.ng Phone:+2348168401851, +2340752420189, +234 92 920 263 Several Data Protection Compliance Organisations (DPCOs) licensed by the National Information Technology Development Agency (NITDA) – list can be found at https://ndpr.nitda.gov.ng/Content/Doc/V.7%20DPCO%20LIST%20.pdf
Scotland	Ken McDonald The Information Commissioner's Office – Scotland Queen Elizabeth House Sibbald Walk Edinburgh EH8 8FT Telephone: 0303 123 1115 Email: Scotland@ico.org.uk
South Africa	Mr. Mosalanyane Mosala The Information Regulator General enquiries: enquiries@inforegulator.org.za
USA	**None**

Appendix 6 - Record of Personal Data and/or Sensitive Personal Data Collected

This form is to be used to identify the staff member(s) who collected Personal Data and/or Sensitive Personal Data. It is to be completed by the **Data Executive** (head of University Department in which Personal Data and/or Sensitive Personal Data are managed).

Personal Data / Sensitive Personal Data	Brief Description (Data)	Source (e.g. Data Subject, organisation, etc.)	Date Obtained (if applicable)	Staff Member who obtained data		Immediate Supervisor	
				Name	Job Title	Name	Job Title

Personal Data / Sensitive Personal Data	Brief Description (Data)	Source (e.g. Data Subject, organisation, etc.)	Date Obtained (if applicable)	Staff Member who obtained data		Immediate Supervisor	
				Name	Job Title	Name	Job Title

Form Completed By:

Name of Data Executive	Job Title of Data Executive	Signature of Data Executive

Date of Completion: _____
dd / mm / yyyy

Date of Next Review: _____
dd / mm/ yyyy

Appendix 7 - Personal Data and Sensitive Personal Data Access list template

This form is to be used to identify the staff members authorised to access specific files or Personal Data and/or Sensitive Personal Data elements. It is to be completed by the **Data Executive** (head of University Department in which Personal Data and/or Sensitive Personal Data are managed) and periodically reviewed at least once per academic year. **Note:** Staff members leaving the department/unit should be ***immediately*** removed from the Access List for that department/unit.

Personal Data / Sensitive Personal Data (File / ERP Module name)	**Brief Description (Data)**	**Location**	**Date Obtained (if applicable)**	**Staff Member with Access**			**Immediate Supervisor**	
				Name	**Job Title**	**Duration of Access**	**Name**	**Job Title**

Personal Data / Sensitive Personal Data (File / ERP Module name)	Brief Description (Data)	Location	Date Obtained (if applicable)	Staff Member with Access			Immediate Supervisor	
				Name	Job Title	Duration of Access	Name	Job Title

Form Completed By:

Name of Data Executive	Job Title of Data Executive	Signature of Data Executive

Date of Completion: _____
dd / mm / yyyy

Date of Next Review: _____
dd / mm/ yyyy

Appendix 8 – Forms

A8.Data Controller Disclosure Form

This form is to be completed by an agent of the University of the West Indies (UWI) when Personal Data is being disclosed to a Non-UWI Data Controller or Data Processor.

This Data Controller form is entered into by *The University of the West Indies (“Data Exporter”)* and the following organisation as *“Data Importer”.*

Data Importer Information

Company Name:	
Address:	
Country:	
Information for Data Protection Officer (or person acting in that capacity)	
Name:	
Job Title:	
Email Address:	
Telephone:	

Data Subject’s Information

Name:	
Address:	
Country:	

Personal Data requested

Who will have access to these Personal Data?

Organisation	Department	Name of individual/Group	Reason for access

The UWI agent providing the information:

Name: _____ Department: _____

Job Title: _____

Signature: _____ Date: _____

Please address and return a copy of this completed form, through the Head of Department / Dean, together with any Supplementary documentation, to:

The University Data Protection Officer

Physical Address:

The University Data Protection Office
Regional Headquarters
The University of the West Indies
2A Hermitage Road
Kingston 7
Jamaica, W.I

Email:

dpo@uwi.edu

Telephone Numbers:

(876) 977-3015 or (876) 970-5417

A8.Data Portability Request Form

Request for Transfer of Data

This form is to be used by the Data subject when requesting Personal Data and/or Sensitive Personal Data to be transferred from The University of the West Indies (UWI) to an external Data Controller or Data Processor.

SECTION 1 – Requestor Details

- This section includes details of the individual / company submitting this request.

- All fields marked as ***** are mandatory.

Are you the Data Subject? *

☐ **Yes**

☐ **No**

If you are the data subject, please enclose evidence of your identity with this form. Acceptable forms of identity are copies of either 1) driver's licence; 2) passport; or 3) birth certificate

SECTION 2 – Data Subject Details

- This section includes details of the individual whose Personal Data and/or Sensitive Personal Data are requested

- A separate form must be completed for each data subject

- All fields marked as ***** are mandatory.

Title:	
Full Name ***** (First and Last)	
Current Address	
Telephone Number:	
Email Address: *****	
Date of Birth:	
Previous Name(s) (if any):	

Previous Address (if at current address for less than 2 years):	

Is/was the Data Subject a UWI employee? *****

☐ Yes

☐ No

Is/was the data subject a UWI student? *****

☐ Yes

☐ No

SECTION 3 – Details of the Request

Who should we provide the requested Personal Data to? *****

☐ Requestor, as indicated in Section 1 above

☐ Data Subject, as indicated in Section 2 above

☐ Other Party

Please provide any relevant information that will help us identify and specifically locate your personal data

SECTION 4 – Declaration (Mandatory)

☐ I am the Data Subject / authorized by the Data Subject named above and hereby request that UWI provide a portable copy of Personal Data, as specified in Section 3 of this form.

I have enclosed the required documents stated in Section 1 above and hereby confirm that all the information supplied in this form is accurate to the best of my knowledge.

Name: _____

Signature: _____ **Date:** _____

Please address and return a copy of this completed form, together with the Supplementary documentation to:

The University Data Protection Officer

Physical Address:

The University Data Protection Office
Regional Headquarters
The University of the West Indies
2A Hermitage Road
Kingston 7
Jamaica, W.I

Email:

dpo@uwi.edu

Telephone Numbers:

(876) 977-3015 or (876) 970-5417

A8.Data Subject Rectification Request Form

According to The UWI Data Protection Policy (2020), you are entitled to request access to and also correct any inaccurate and/or incomplete information held for you by the University. This form must be completed in order for the University to process your request.

We will respond to your request promptly, but in at least 30 (thirty) days, with:

- confirmation of your request; and
- notice of any further information we may require from you to enable compliance with your request.

Please note the following:

- depending on the complexity and number of requests we receive, we may extend the period by a further two (2) months;
- the information you provide will be used for the purpose of identifying you and the Personal Data requested.

Section A: Requestor Details (Mandatory Section)

Are you the Data Subject?

☐ **Yes**

☐ **No** (You will need to enclose Data Subject's written authority certified by a Justice of the Peace or Notary Public)

Your Name (Last, First):	
Id number:	
Id Type: (E.g. Passport, DL, UWI Id)	
Contact telephone number:	
Email Address:	
Physical Address	

Section B: Details of Data Subject (if different from Requestor)

Your Name (Last, First):	
Id number:	
Id Type: (E.g. Passport, DL, UWI Id)	
Contact telephone number:	
Email Address:	
Physical Address	

Section C: Description of information to be rectified (corrected or completed)

Notes:

- The University reserves the right to deny rectification if such rectification conflicts with local legislation or University Regulations.
- Certified copies of documents verifying the **correct** form of the information to be rectified must be provided along with this completed form **before** rectification can considered.

Section D: Declaration

I, _____ do hereby,

First Name Last Name (e.g. John Doe)

1. **Confirm** that I have read and understood the terms of this **Data Subject Rectification Request Form;**

   In relation to this request

2. **Consent** to the processing of the Personal Data and/or Sensitive Personal Data submitted on this form as well as any Personal Data which I submit in the future;

3. **Consent** to the sharing of my Personal Data and/or Sensitive Personal Data and, where the request relates to someone else, their Personal Data and/or Sensitive Personal Data, with the Supervisory Authority in any jurisdiction which governs the University at the location where the processing of Personal Data is to take place;

4. **Consent** to the sharing of my Personal Data and/or Sensitive Personal Data and, where this request relates to someone else, their Personal Data and/or Sensitive Personal Data, with other Data Controllers and/or Data Processors, who obtained the Personal Data from the University, or publicly as a result of that Personal Data being made public by the University, to rectify this Personal Data;

5. **Certify** that the information provided in this request is true, correct and within my personal knowledge; and

6. **I understand** it is necessary to confirm my identity and, if applicable, that of the Data Subject on whose behalf I am acting.

_____ _____

Signature **Date**

Supplementary Documentation

- Proof of Requestor's identity (*See* Section A)
- Proof of Data Subject's Identity (*See* Section B)
- Written Authority from Data Subject (*See* Section A)
- Proof supporting need for rectification (*See* Section C, Notes - second bullet 2)

Please address and return a copy of this completed form, together with the Supplementary documentation to:

The University Data Protection Officer

Physical Address:

The University Data Protection Office
Regional Headquarters
The University of the West Indies
2A Hermitage Road
Kingston 7
Jamaica, W.I

Email:

dpo@uwi.edu

Telephone Numbers:

(876) 977-3015 or (876) 970-5417

A8.Possible Personal Data and/or Sensitive Personal Data Breach - Incident Report

Details of Incident	To be completed by head of area (Unit/Department/School/Faculty/Division) or, in the case of contractors, University contact			
1. When was the incident discovered? *(Date)*	Date:			
2. When did the incident take place? *(Date)*	Date:			
3. Where was the incident? *(Location of incident - area, location within area)*	Area: Location within area:			
4. Who made you aware of the incident (Name; Position)	**Name**	**Email Address**		**Position**
5. Was an email, stating that an incident took place, sent to the DPO? (Y/N)				
6. If "yes" to 5, when was this email sent? (Date/Time)				
7. Your information *(Name, Email address, telephone number, Office address)*	**Name**	**Email Address**	**Office Address**	**Telephone Number**
8. Description of Incident				

9. What, if any, ICTs (devices, software) were involved in the incident?	
10. What types of records were involved? (Grades, Health records, Student bio info., etc.)	
11. How many Data Subjects were affected?	
12. Whose records were involved? (Full names of individuals, Id numbers of individuals)	
13. Was action taken when the incident was discovered? (Y/N)	
14. What, if any, action was taken? (Brief description)	
15. If action was taken, who took it? (Name, Email address, telephone number, Office address)	

Page intentionally left blank.

A9.Personal Data Request Procedures

March 2021

A9.1. Introduction

As defined in The UWI Data Protection Policy (p.6), **Personal Data** are data which relates to a *living* individual or to an individual who has been *deceased for less than thirty years*, who is, or can be, identified, either from the data or from the data in conjunction with other information, which is in, or is likely to come into the possession of, the Data Controller. Personal Data include photographs, audio and video recordings, and text messages. The **Data Controller** is a person who (either alone or with others) controls the contents and use of Personal Data. The UWI, as a 'legal person', is a Data Controller.

These Procedures are complementary to The UWI Data Protection Policy and prescribe how requests for Personal Data are to be managed. These Procedures are applicable to all requests - those made by staff, students, or external entities - irrespective of the use to be made of the data.

A9.2. Authority

These Procedures have been approved by the University Finance and General Purposes Committee – a sub-committee of University Council – for implementation at all campuses of The UWI.

A9.3. Penalties for Breach

Staff who breach these procedures are subject to disciplinary procedures as outlined in the relevant University Regulations *(for additional information, see section 4 – The UWI Data Protection Policy)*.

A9.4. Roles and Responsibilities

This section defines the roles and responsibilities involved in the management of personal data requests.

A9.4.1 Data Executive

The **Data Executive** is the head of a University department in which Personal Data are managed – collected, stored, processed, and/or maintained. The Data Executive is responsible for approving requests for Personal Data but may delegate such responsibility to, or seek assistance from, one or more Data Custodian (see A9.4.2).

The Data Executive shall be responsible for establishing the criteria for sharing Personal Data and ensuring that existing Data Custodians are kept abreast of these criteria, and that new Data Custodians are introduced and become fully *au fiat* with them before assuming duties. The Data Executive shall also ensure that staff joining the department are fully aware of both these Procedures and the established criteria for sharing Personal Data.

Examples of Data Executives: Director, HRMD (or equivalent); Manager, Payroll (or equivalent); Assistant Registrar and/or Senior Assistant Registrar, Admissions; Assistant Registrar and/or Senior Assistant Registrar Exams.

A9.4.2 Data Custodian

A **Data Custodian** manages the actual **data**. Data Custodians are responsible for, among other things:

i. ensuring and maintaining the accuracy, integrity, and privacy of Personal Data;
ii. granting or denying requests for Personal Data (on behalf of the Data Executive) *(see* A9.4.1
iii. reviewing requests for Personal Data and responding within a reasonable time
iv. assisting individuals and entities (external and UWI sub-entities) with identifying what is required to fulfill their request for Personal Data
v. Interfacing with Enterprise Systems Support (see A9.4.4) for requests that they are not able to fulfill without additional support

A9.4.3 Data Requestor

A Data Requestor is any individual (staff, student, external entity) who makes a request for Personal Data.

A Data Requestor whose request has been approved by a Data Executive/Data Custodian must use the data only in a manner consistent with purposes approved by the University.

A Data Requestor should not share Personal Data with others who do not have approval to use that same data unless explicitly authorized as part of the request for Personal Data.

A Data Requestor must follow any instructions or restrictions imposed by the Data Custodian or Data Executive.

A9.4.4 Enterprise Systems Support (ESS)

Enterprise Systems Support (ESS) are ICT staff who work in any section which supports the University's Enterprise Systems.

ESS are responsible for fulfilling requests for Personal Data which cannot be handled solely by the Data Executive/Data Custodian.

ESS will fulfill these requests by pulling the required data from the various Enterprise Systems (e.g. PeopleSoft, Banner) and passing it on to the Data Executive/Data Custodian in the required format.

ESS can only fulfill requests which have been approved by the Data Custodian (or Data Executive).

A9.5. Procedures - Personal Data Request

A9.5.1 Who is authorized to make a request for Personal Data?

A Personal Data request may come from an individual, University department or an external entity (Auditors, Government, Unions, Alumni, etc.).

A9.5.2 Identifying the person/entity making the request for Personal Data

i. Before responding to a Personal Data request, the relevant Data Custodian (or Data Executive) shall take reasonable steps to verify the identity of the person or entity (sub-entity) making the request.

ii. Where the Data Custodian (or Data Executive) is unable to verify the identity of the requestor, the Data Custodian (or Data Executive) may ask the requestor to provide additional information to confirm his or her identity.

A9.5.3 To whom should a request for Personal Data be made and how might it be made?

i. Requests for Personal Data shall be made to the relevant Data Custodian or Data Executive.
ii. Requests for Personal Data made to the relevant Data Custodian shall be copied to the relevant Data Executive.
iii. Requests for Personal Data, made to either a Data Custodian or a Data Executive, shall be in writing.

   - Oral requests made, even if the requestor is a direct supervisor of the Data Custodian or Data Executive shall not be entertained
   - **Note:** A Data Custodian and/or Data Executive shall be in breach of these Procedures if he or she fulfils an oral request which is not supported by a written request. This support shall be either simultaneous or within 24 calendar hours

iv. Requests for Personal Data to either a Data Custodian or Data Executive shall use the prescribed form (See Appendix I – Prescribed Forms).
v. Once the form has been completed, and the request approved, it can then be forwarded to Enterprise Systems Support for fulfillment, if required.

A9.5.4 How to handle improperly submitted requests for Personal Data

Where a request for Personal Data is made directly to a member of ESS and does not come from a Data Custodian or Data Executive, such a request shall be forwarded to the appropriate Data Custodian or Data Executive for approval.

A9.5.5 Limitations

- Data Custodians shall provide Personal Data to only those Data Requestors who have a need for the data in compliance with The UWI Data Protection policy.

- If a personal data request is complex or the individual has made several requests, ESS may extend the period of fulfillment by a time agreed on with the Data Custodian. The Data Custodian shall, within a reasonable time from the receipt of the request, inform the Data Requestor of the extension and explain why the extension is necessary.

A9.5.6 Response to request for Personal Data

The relevant Data Custodian (or Data Executive) shall confirm receipt of the request for Personal Data within 24 hours. This confirmation shall include:

- Date (and time) the request was received
- The due date to produce the data requested. This will be negotiated based on the urgency of the data, the complexity of the request and the present workload of staff who will fulfill the request.

It is important that when a request is made, the Data Custodian (or Data Executive):

i. is very clear on what data are required;
ii. has knowledge as to whether the required data are available;
iii. fully understands the purpose/reason for the data so as to convey this to Enterprise Systems Support (if necessary);
iv. the urgency of the data.

A9.5.6.1 What to do when you have fulfilled a personal data request (ESS)

Once a request for Personal Data has been fulfilled:

i. the data should be sent, in the required format, to the Data Custodian (or Data Executive);
ii. the Data Custodian (or Data Executive) will then forward the data to the Data Requestor.

A9.5.6.2 Denying a personal data request

The Data Custodian (or Data Executive) may deny a Personal Data request where even after requesting additional information, Data Custodian (or Data Executive) is still not able to identify the Data Requestor making the Personal Data request.

The Data Custodian (or Data Executive) may also deny a Personal Data request if it is determined that the purpose for which the data is requested is in breach of the University's Data Protection policy.

In instances where a request for Personal Data is denied, the Data Custodian (or Data Executive) shall inform the Data Requestor no later than 2 days after receiving their request. The response from the Data Custodian (or Data Executive) should provide: the reason(s) the request could not be honored.

Appendix A9.9.I – Prescribed Forms

Personal Data Request Form

The following form should be used for all requests for Personal Data, in relation to yourself, a staff member or student, or past staff member or student or other UWI affiliate. Please complete each section carefully as required. Incomplete forms cannot be processed.

Section I ***(to be completed by Data Requestor)*** *You should only use this data for the purpose stated in this request. Failure to abide by the terms under which access to this data was granted may result in disciplinary action taken against you.*

Title: Prof □ **Dr** □ **Mr.** □ **Mrs.** □ **Ms.** □ **Miss** □ **Other**_____

CONTACT INFORMATION	
Date Requested:	
Name of Requestor:	
Department/Organization:	
Email address:	
Phone number:	
ID number (where applicable)	

About whom are you requesting information?

- □ Myself
- □ Student
- □ Staff
- □ Alumni
- □ Other Please specify _____

Description of Request: (Attach supporting documentation if necessary)

Purpose: (what will the data be used for)

Priority: High ☐ Low ☐

If High, please explain

Recipients: (who else will be given access to this data)
All persons who are given access will be personally accountable for the data.

Name:

Email address	Phone number	Department/Organization	Reason for access

Name:

Email address	Phone number	Department/Organization	Reason for access

Name:

Email address	Phone number	Department/Organization	Reason for access

Name:

Email address	Phone number	Department/Organization	Reason for access

Name:

Email address	Phone number	Department/Organization	Reason for access

Due Date: …….. **Signature of Requestor: ……..**

Office Use Only

Staff member assigned:
Request received on the …… day of …… 20.....
Additional information received on the ……..day of ……. 20……
Request approved on the ……..day of ……. 20……
Request denied on the ……..day of ……. 20……
Response sent on the ……..day of ……. 20……

Reasons for request being denied

…… ……

Data Executive **Date**

Section II ***(to be completed by Data Executive/Data Custodian)***

Details of data required: (specific criteria to be used)

Specific columns to be reported: (attach sample report layout if necessary)

File Format: PDF ☐ Excel ☐ Word ☐ Other: (please specify) ☐

Section III ***(to be completed by ESS)***

Staff Member Assigned: ☐ Date completed: ☐

Comments: (Any issues, limitations, errors that were found)

DATA REQUEST DENIAL

Pursuant to The UWI Data Protection Policy

Your request made on the day of has been denied for the following reasons:

…… ……

Data Executive **Date**