



THE UNIVERSITY OF THE WEST INDIES

STAFF PRIVACY STATEMENT

The University of the West Indies (“The UWI”, “University”), as an employer, has certain legal, contractual and administrative obligations. In discharging these obligations, we are committed to ensuring the privacy of your information. We are dedicated to upholding the highest standards of data protection and confidentiality, ensuring that your personal information remains secure and confidential. This Statement contains the practices to be followed by The University of the West Indies pertaining to the collection, use and disclosure of your Personal Data in accordance with our Data Protection Policy.

1. For the purpose of this Statement:

“Personal Data” means data 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 or from the data in conjunction with other information, which is in, or is likely to come into the possession of The UWI. It includes information in the form of photographs, audio and video recordings, and text messages.

“Sensitive personal data” refers to personal data that includes any of the following information regarding a data subject: genetic data or biometric data; filiation, racial or ethnic origin; political opinions, philosophical beliefs, religious beliefs, or other similar beliefs; membership in any trade union; physical or mental health or condition; sex life; the alleged commission of any offense by the data subject or any proceedings for any offense alleged to have been committed by the data subject.

To whom does this Statement apply?

2. The rights and obligations outlined in this Statement will apply to all past and present staff of the University, including trainees and contractual workers of the UWI. All members of Staff must comply with the policies, procedures and practices outlined in this Statement.

What Personal Data we process and why?

3. We collect and use your personal data for various purposes related to your employment with the University. These purposes include managing your employment, providing benefits, monitoring your performance, ensuring accurate payments, offering training, and complying with legal obligations. Additionally, we have a legitimate interest in holding emergency contact information. It's important to note that if we use your data for research, it will only be done in anonymized forms to prevent identification and to comply with our legal obligations.
 - 3.1 Personal information comprises various details, including your name, photograph, employee username, ID number, date of birth, gender, nationality, National Insurance (NI) number, and copies of documentation proving your right to work, such as your passport or visa. Contact details are also part of this category.
 - 3.2 Job-related information includes your role title, department, information about your employment contract (e.g., start date, hours, contract type, and salary), details of any benefits you've received, and records of periods of leave taken including holidays, sickness absences, various types of leaves and sabbaticals. Your financial details are collected to pay your salary and expenses and respond to requests from external entities like financial institutions for loan applications. We also ensure compliance with general labour employment legislation.
 - 3.3 Performance information includes assessments of your performance, which include appraisals, performance reviews, ratings, training participation records, performance improvement plans, promotions, discipline, probation and details of any disciplinary or grievance procedures in which you have been involved. This category also covers any warnings issued to you and related correspondence.
 - 3.4 Education and work history includes details about your qualifications, skills, experience, employment history, and references provided and received. Additionally, it may include information about proposed or undertaken research projects.

- 3.5 Information related to your family, lifestyle, or social circumstances may be collected in specific situations. For instance, we may gather limited information about your spouse, partner, children, civil partner, or other individuals if you name them as emergency contacts or when shared parental leave is requested.
- 3.6 The collection of Personal Data begins from your first interaction with The UWI. Data may also be obtained from third parties such as referees, previous employers, or other relevant sources.

How will we use your Personal Data?

4. The UWI collects, maintains, and uses personal data, including sensitive personal data, of staff members and contractors solely for the intended purposes communicated at the time of original collection. These purposes facilitate the administration of your employment or engagement with the University and include aspects such as recruitment, development, safety, reward, security, equal opportunities, and welfare. The UWI also ensures lawful processing of staff data post-employment and acknowledges its obligations to maintain the confidentiality and integrity of all personal data in its possession.

Will we be sharing your Personal Data with anyone?

5. If your Personal Data is to be relayed to a third party, outside the original purpose for which it was collected and about which you were informed, we will obtain your written consent before disclosing the Personal Data.

Who will have access to your Personal Data?

6. In the course of their normal and reasonable duties, designated University personnel will have access to the Personal Data of staff. This access to your Personal Data will not exceed that which is necessary for accomplishing the initial purpose for which it was collected. The University will identify persons who have the authority to access your Personal Data through the appropriate channels.
7. The University is committed to ensuring the security of personal data by utilizing the appropriate technical and organizational measures that have been implemented to prevent unauthorized access, disclosure, alteration, or destruction of personal data.

How do we get your Personal Data?

8. Data may be collected in the following ways:
 - i. Directly from you.
 - ii. From your previous employer (where applicable).
 - iii. From referees – either generally or for purposes of evaluation and promotion.
 - iv. From other sources not identified in i-iii (above), such as, captured from video recordings or photos of a meeting you attended – online or face-to-face.

Why is personal information from video surveillance collected?

9. The UWI operates video surveillance (aka CCTV) systems across its various locations. These systems are operated to ensure your safety and for the prevention and detection of security incidents. Video surveillance is deployed in specific areas, which may include entrances, exits, common areas, and other locations where security is of concern. This video surveillance data will include visual images of individuals as well as a time and date stamp of the recordings.

How long do we keep your Personal Data?

10. Any Personal Data collected by the University will be retained during the period of active employment as well as after the employment period, within the confines of the original purpose for which the data was collected, subject to The UWI's Records Management Policy. These purposes include but are not limited to operational purposes as well as to legal or regulatory purposes, or for the establishment, exercise, or defense of legal claims.

How can I raise concerns about the processing of my Personal Data?

11. For purposes of the protection of your Personal Data, The University has appointed a *Data Protection Officer*. If you have any feedback or concerns in relation to the processing of your Personal Data, please contact the University Data Protection Officer at dpo@uwi.edu.

Rights of Access and Correction

12. You have the following rights:

Version Number: 0.5

Version Date: January 16, 2024

Version Status: Draft – For Approval by Data Protection Policy Project Implementation Committee

- i. the right to fair processing of information and transparency over the use of your Personal Data by the University;
- ii. the right to have any mistakes in your Personal Data held by the University corrected; and
- iii. the right to have certain Personal Data erased or restricted (under prescribed circumstances).
- iv. the right to be informed about what personal data is being collected, why it is being collected, and how it will be used;
- v. the right to consent to the collection (or further processing of your Personal Data); and
- vi. the Right to Access/ to request access to your personal data held by the University. This includes the right to obtain a copy of your Personal data and information about how it is being used.

You may request the erasure of your Personal Data

13. You may ask us to delete or remove your Personal Data if:

- i. there is no good reason for us to continue processing your Personal Data;
- ii. you believe we may have processed your Personal Data unlawfully; or
- iii. we are required to erase your Personal Data to comply with the law.

Please note that we may not be able to comply with your request for specific legal and operational/administrative reasons, which if applicable, you will be notified.

You may object to processing of your Personal Data

14. You may object to the processing of your Personal Data if you believe that this processing impacts your fundamental rights and freedoms. Keep in mind however, that these may be overridden on grounds of public interest or legitimate interest.

Deceased Individuals

15. The rights outlined in this Statement will extend to deceased individuals and their estate.

Compliance with Privacy Policy

16. All University staff members must comply with this Statement. Any breach of this Statement will constitute grounds for disciplinary action.

Changes to this Notice

17. The University reserves the right to update or amend this Notice at any time. Any changes will be communicated through appropriate channels.

18. This Notice is effective as of January 1, 2024, and will be reviewed annually. For more information, please visit our website or contact our Data Protection Officer.