Williams & Wilson

DATA PROTECTION POLICY

Williams & Wilson Limited
(the "Company")

GLOSSARY OF TERMS

TERM	MEANING
ADM	Decision making based solely on Automated Processing or Profiling resulting in a legal effect or otherwise significantly affects a Data Subject.
Automated Processing (Profiling)	Using Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
GBC1	Williams & Wilson Limited
Board	Board of directors of the Bank
Controller	The person or organisation that determines when, why and how to process Personal Data.
Criminal Convictions Data	Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.
Data Protection Legislation	Mauritian data protection legislation and all other legislation and regulatory requirements in force from time to time in any of the aforementioned countries or any other country which apply to the Bank relating to the use of Personal Data (including, without limitation, of Act 20 - The Data Protection Act 2017 for Maurtius and any guidance and codes of practice issued by the relevant data protection or Supervisory Authority.
Data Subject	A living identified or identifiable individual about whom we hold Personal Data.
DPIA	Data Privacy Impact Assessment as defined in section X
DPO	Data Protection Officer
Global	Global
Executive Management	**WILLIAMS & WILSON** Executive Directors and the term Executive shall apply to any Executive Director as indicated
GDPR	General Data Protection Regulation 2016/679
Personal Data Breach	Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data
Privacy Guidelines	The company's privacy related guidelines to assist in interpreting and implementing the Policy and Related Policies.
Privacy Notice	General or specific notices setting out information required by law to be provided to Data Subjects.
Pseudonymised Personal Data	Personal Data which has been replaced with one or more artificial identifiers or pseudonyms so that the Data Subject cannot be identified without the use of additional information which is kept separately and

	Secure by the company.
Senior Info/Cybersec Mgr	Senior Information and Cyber Security Manager
Special Categories of Personal Data	Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. The Bank will also treat Criminal Convictions Data as if it is Special Category Personal Data.
Staff	Directors and employees, whether permanent or temporary, individual contractors, consultants, agency and other workers.
Supervisory Authority	Mauritian Data Protection Commission and any other applicable data protection or supervisory authority

1. INTRODUCTION

Williams & Wilson Limited ("we", "us", "our", the "Bank" and **W&W**) recognises and respects the fundamental rights of individuals to privacy as enshrined by law. We will uphold all data protection laws of the jurisdictions in which we operate, being Mauritius. However, we remain bound by Mauritian laws, and this Policy is based primarily on, the Data Protection Act 2017, the Act repeals and replaces the Data Protection Act 2004, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR).

This Policy sets out how we handle the Personal Data of our customers, clients, directors, employees, consultants, contractors, interns, agency workers and other third parties (together "Data Subjects").

By "Personal Data" we mean any information identifying an individual or information relating to an individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers that we possess or can reasonably access. Personal Data includes **Special Categories of Personal Data** and **Pseudonymised Personal Data** (*see Glossary of Terms*) but excludes anonymous data or data that has had the identity of an individual permanently removed. The term "Personal Data" is widely applied, and can be factual (for example, a name, email address, location or date of birth) or an opinion about a person's actions or behaviour.

2. APPLICATION

The Policy applies to ***all*** Personal Data that we process. By "processing", we mean any activity that involves the use of Personal Data including, without limitation, collecting, recording, holding or storing Personal Data, or carrying out any operation on such data, such as organising, amending, retrieving, using, sharing, disclosing, erasing or destroying it and also, transmitting or transferring Personal Data to third parties. The Policy applies regardless of the media on which the Personal Data is held or whether it relates to past or present employees, workers, customers, clients or supplier contacts, website users or any other Data Subject.

Further, the Policy applies to all **W&W's** directors and employees, whether permanent or temporary, individual contractors, consultants, agency and other workers ("you", "your" and together "Staff"). You must read, understand and comply with this Policy when processing Personal Data on our behalf and attend any training on its requirements.

3. COMPLIANCE WITH THIS POLICY

This Policy sets out what we expect from you in order for the company to comply with applicable law. Your compliance with this Policy is mandatory. It, together with Related Policies and Privacy Guidelines are available to you on Policy Hub or, via other means, to help you interpret and act in accordance with this Policy. You are also required to comply with Related Policies and Privacy Guidelines. A breach of this Policy may result in disciplinary action including, if appropriate, termination of our relationship with you.

4. ROLES AND RESPONSIBILITIES

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Bank and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Listed in Art. 83(5) GDPR, the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year

W&W is registered as a Controller with the Mauritian Data Protection Commission under registration id: GB22201242.

The Policy is reviewed by our legal department and approved by the **Board** every two years or more frequently, if the need arises e.g. due to a change in law.

Executive Management, General Managers and Heads of Department are responsible for ensuring all Staff in their respective teams comply with this Policy and shall need to implement appropriate practices, processes, controls and training to ensure that compliance.

The **DPO** is responsible for overseeing this Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Vuk Trajkovic, email legal@williamsandwilson.org . Please contact the **DPO** with any questions about the operation of this Policy or Data Protection Legislation generally or if you have any concerns that this Policy is not being or has not been followed.

5. PERSONAL DATA PROTECTION PRINCIPLES

All processing of Personal Data by the Bank shall comply with the seven (7) Principles set out in Data Protection Legislation, specifically **GDPR**, which require Personal Data to be:

5.1 **Processed lawfully, fairly and in a transparent manner** (**Lawfulness, Fairness and Transparency**): **W&W** shall:

- only collect, process and share Personal Data where the Bank has a legal basis (**Legal Basis**) under Data Protection Legislation, for doing so.
- only use Personal Data in a way that is fair and shall not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- clear, open and honest with people from the start about how the Bank will use their Personal Data.

These restrictions are not intended to prevent or prohibit the processing of Personal Data by you, but rather, they ensure that the Personal Data we process is done so fairly and without adversely affecting Data Subjects.

Typically, the company processes Personal Data on the following **Legal Bases** set out under Article 6 of the **GDPR (**and in so doing, the Bank adheres to the requirements of lawfulness and fairness):

(a) where this is necessary for the performance of a contract with the Data Subject e.g. a contract of employment or for services and when opening customer account or providing other banking services subject to our terms and conditions;

(b) to meet our legal compliance obligations arising otherwise than by virtue of a contract, e.g. to meet our reporting obligations to **MFSC**, or to file a suspicious activity report with the National Crime Agency;

(c) to protect the Data Subject's vital interests – this legal basis will only be applied rarely in circumstances involving the need to protect the life of a Data Subject e.g. medical emergency evacuation of a member of Staff;

(d) where this is necessary for the performance of a task carried out in the public interest;

(e) to pursue our legitimate interests for purposes (where these are not overridden by the interests or fundamental rights and freedoms of Data Subjects).

Generally, the company ***does not*** process Personal Data on the basis of the "**consent"** of Data Subjects and you should usually rely on another **Legal Basis** for your proposed processing. Where you determine consent to be the only appropriate **Legal Basis** for processing this data, you should ensure that this consent is explicit, specific to the purpose and freely given by the Data Subject and, finally that this consent is capable of being withdrawn. In certain circumstances, **W&W** may be unable to provide services or continue with a relationship, where the Data Subject has refused to or withdrawn their consent to the processing of their Personal Data. In such circumstances, the matter must be referred to the **DPO** who in turn, will escalate the matter appropriately.

Where the company does not have a **Legal Basis**, it will not process the Personal Data.

In certain circumstances e.g. background employment screening, compliance screening for financial crime risks for customers, counterparties and suppliers and **KYC**, **W&W** will process Special Category Data or Criminal Convictions Data. **W&W** must have a **Legal Basis** under Article 6 **GDPR** to process this data and satisfy one of the conditions in Article 9 **GDPR** in addition to the requirements under Mauritius regulates data protection under the Data Protection Act 2017 (DPA 2017 or Act). The **GDPR** Article 6 Legal Bases typically relied upon by **W&W** when processing Special Category Data and Criminal Convictions Data are (i) to enter into a contract with the Data Subject; (ii) to meet our legal compliance obligations arising by virtue of law e.g. compliance with Anti-Money Laundering Regulations; and (iii) the processing is in our or a 3rd party's legitimate interest. **W&W** will rely on the following **GDPR** Article 9 conditions for processing this data: (i) employment, social security and social protection purposes; and (ii) reasons of substantial public interest. In each case, **W&W** must be authorised by law to rely on the **GDPR** Article 9 conditions by Schedule 1 **DPA2017. W&W** will not generally process this type of data based on consent and should, where possible, seek to rely on an alternative **Legal Basis**.

DPA2017 requires that we have "an appropriate policy" in place to cover any processing of Special Category Data or Criminal Convictions Data and this Policy constitutes W&W's "appropriate policy".

In compliance with the requirement for transparency, an appropriate **Privacy Notice** shall be given to the Data Subjects at the time of collection of the Personal Data. This may be a general notice or one which covers processing relating to a specific purpose and may contained in another document e.g. account opening form or even be given orally, if appropriate. See Privacy Guideline on Privacy Notices.

During our relationship with the Data Subject, we shall notify the Data Subject of any changes to any relevant Privacy Notice by sending the revised Notice to the Data Subject or otherwise publishing this on our website and notifying Data Subjects accordingly.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we shall provide the Data Subject with all the information required by Data Protection Legislation via the appropriate **Privacy Notice** and shall check that the Personal Data was collected by the third party in accordance with Data Protection Legislation and on a basis which contemplates our proposed processing of that Personal Data.

5.2 Collected only for specified, explicit and legitimate purposes (Purpose Limitation):

You must only collect Personal Data for specified, explicit and legitimate purposes. It must not be further used or otherwise processed in any manner incompatible with those purposes.

The company shall not and accordingly you cannot use Personal Data for new, different or incompatible purposes from that originally disclosed to the Data Subject when it was first obtained *unless* you have informed the Data Subject of the new purposes.

Should a change in purpose be contemplated, the company's relevant Privacy Notices shall be updated appropriately. See Privacy Guidelines on Processing Purpose Changes.

5.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation):

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You may only process Personal Data when performing your job duties requires it. You cannot process Personal Data for any reason unrelated to your job duties. You may only collect the Personal Data that you require for your job duties and this shall not be excessive e.g. where circulating details of a prospective job candidate to **W&W** interviewers, circulating details of the candidate's home address may be considered excessive. Staff shall at all times ensure any Personal Data collected and processed is adequate and relevant for the intended purposes. See Privacy Guideline Handling Personal Data.

Where Personal Data is no longer needed for specified purposes, it shall be, deleted or otherwise anonymised in accordance with the Bank's Record Retention Policy and Procedures.

5.4 Accurate and where necessary kept up to date (Accuracy):

Personal Data must be accurate and, where necessary, kept up to date. Staff shall ensure that all Personal Data is corrected or deleted without delay when inaccurate. You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data including, if appropriate, requesting Data Subjects to check and ensure that the data we hold about them is accurate and up to date.

5.5 Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation):

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. **W&W** maintains a Record Retention Policy and Procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time. You must comply with the Bank's Record Retention Policy and Procedures.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for our legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

You will take all reasonable steps to destroy or erase from our systems (save for any back up storage files) all Personal Data that we no longer require in accordance with all the Record Retention Policy and Procedures. This obligation includes requiring third party processors including vendors to delete that data, where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

5.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality):

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosur

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it;

(b) **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) **Availability** means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Information Security Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with Data Protection Legislation and relevant standards to protect Personal Data and the Bank's data generally.

5.7 Transferring of Data to another country:

A controller or processor may transfer personal data outside Mauritius if the DPC is provided with proof confirming that there are appropriate safeguards in place for the protection of personal data. Personal data may also be transferred outside Mauritius if, prior to such transfer, the data subject has been informed of any possible risks of the transfer and the data subject has given explicit consent to the transfer. If the controller or processor cannot provide for the appropriate safeguards in relation to the transfer of personal data to another country, the controller or processor, as applicable, must obtain the prior authorization of the DPC.

The transfer may also take place if it is necessary for the performance of a contract between the data subject and the controller, or for the taking of steps at the request of the data subject with a view to them entering into a contract with the controller.

The transfer of personal data to another jurisdiction can also be allowed on such terms as the DPC may approve for the protection of the rights of the data subjects. The DPC has the power to suspend or prohibit the transfer of data to another jurisdiction if the processor or controller is not able to demonstrate either the effectiveness of safeguards or the existence of compelling legitimate interest.

In addition, under the Guidelines on Outsourcing by Financial Institutions (revised in March 2018) (the BOM Outsourcing Guidelines) issued by the Bank of Mauritius (BOM), a financial institution must strictly adhere to the Act and ensure when storing customers' information on the cloud. The BOM Outsourcing Guidelines impose a series of conditions for the implementation of cloud-based services by financial institutions. As such, financial institutions should ensure that they are in possession of a certificate of conformity from a law practitioner certifying that the systems in place comply with data protection and other applicable laws.

5.8 Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests):

Data Subjects have legally enforceable rights when it comes to how we handle their Personal Data. These include the right to:

(a) withdraw consent to processing at any time;
(b) receive certain information about our processing activities;
(c) request access to their Personal Data that we hold;
(d) prevent our use of their Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict processing in specific circumstances;
(g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) object to decisions based solely on Automated Processing, including profiling (ADM);
(i) prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
(j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
(k) make a complaint to the **MDPC** or other applicable Supervisory Authority; and
(l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

W&W shall always inform Data Subjects of their legal rights via an appropriate Privacy Notice and further, shall respond to requests by Data Subjects exercising their legal rights (**Data Subject Requests**). W&W shall do so within the statutory time limits, if any and in the manner prescribed by Data Protection Legislation.

Before responding to any Data Subject Request, you must verify the identity of the individual making the request in order to minimise the risk of a third party persuading you into disclosing Personal Data without proper authorisation.

Guidance and training shall be provided to Staff to ensure that Staff are able to recognise a **Data Subject Request** and deal with it appropriately and within the statutory prescribed deadlines. Data Subject rights are not absolute, and in certain circumstances, **W&W** may refuse to comply with a **Data Subject Request.** Staff must comply with the companies Data Subject Request Procedures and relevant Privacy Guideline in this respect and attend any relevant training provided by the Bank from time to time.

5.9 **By law, WILLIAMS & WILSON is responsible for and must be able to demonstrate compliance with the data protection Principles (Accountability)**.

WILLIAMS & WILSON shall put in place appropriate technical and organisational measures which are subject to continuous improvement, to ensure compliance with the data protection Principles and shall ensure adequate resources and controls are in place for this purpose and to document compliance with Data Protection Legislation including:

(a) As a matter of good practice and not a legal requirement, appointing a suitably qualified **DPO** and an Executive **(DCEO & COO**) accountable for data privacy;

(b) implementing Privacy by Design when processing Personal Data. To this end:

- ☐ We shall consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- ☐ We shall make data protection an essential component of the core functionality of our processing systems and services.
- ☐ We shall anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals.
- ☐ We shall only process the Personal Data that we need for our purposes(s), and that we only use the data for those purposes.
- ☐ We shall ensure that Personal Data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- ☐ We shall provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- ☐ We shall adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their Personal Data.
- ☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- ☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- ☐ When we use other systems, services or products in our processing activities, we shall make sure that we only use those whose designers and manufacturers that take data protection issues into account.

☐ We shall use privacy-enhancing technologies to assist us in complying with our data protection by design obligations.

Data Protection Privacy Assessment

In compliance with Privacy by Design, you should always assess what measures, if any, can be implemented on all Bank programmes, systems or processes that involve the processing of Personal Data. You **must** conduct a **DPIA** when implementing major system or business change programs involving the processing of Personal Data including when you propose to:

- use new technologies (programs, systems or processes), or change technologies (programs, systems or processes);
- Automated Processing including profiling and **ADM**;
- large-scale processing of **Special Category Personal Data** or **Criminal Convictions Data**; and
- large-scale, systematic monitoring of a publicly accessible area e.g. our Banking Hall.

The **DPIA** process helps you to identify and minimise data protection risks of your project. Refer to the Privacy Guideline on **DPIA**s and use any assessment tools provided by the Bank to undertake your assessment.

(d) regularly training Staff on this Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, **DPIA**s and Personal Data Breaches. The Bank shall maintain a record of training attendance by Staff; and

(a) where appropriate, regularly testing via our Compliance Monitoring Programme, of the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

6. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

W&W'**s** activities do not involve **ADM,** which is prohibited by **MDPC** for example, unless certain requirements are met. The Bank uses **Automated Processing** for a number of its activities e.g. automated compliance screening such as Accuity, and data generated by this processing is reviewed and analysed by Staff prior to a decision being made which has a legal or may have a significant effect on an individual concerned.

7. DIRECT MARKETING

W&W currently does not undertake electronic direct marketing activities for which a Data Subject's prior consent is required (e.g. via email, text or automated calls). The limited exception for existing customers known as "soft opt-in" shall be available to the Ban allowing us, if required, to send marketing texts or emails only if we have obtained contact details in the course of providing a type of banking service to that person, we are marketing other similar services, and we give the person an

opportunity to opt out of marketing when first collecting their details and in every subsequent message to that person. To the extent that the Bank engages in direct marketing at any time, it shall comply with the requirements of Data Protection Legislation generally including those relating to consents, the Data Subject's right to object, and customer preferences including the suppression of Personal Data where a customer opts out of direct marketing.

8. SHARING PERSONAL DATA

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, director, agent or representative of Williams & Wilson that is, if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the Privacy Notice provided to the affected Data Subject;
(c) the third party has agreed to comply with **W&W**'s data security standards, policies and procedures otherwise has its own which are satisfactory to **W&W**, and has put adequate security measures in place;
(d) the transfer complies with any applicable cross-border transfer restrictions; and
(e) a fully executed written contract that contains **MDPC** -approved third party clauses has been obtained.

7. RECORD OF PROCESSING ACTIVITIES

Data Protection Legislation requires us to keep full and accurate records of all our Personal Data processing activities. The Bank shall maintain a written record of all its processing activities via a departmental specific Record of Processing Activities (**Record**) stored on SharePoint or similar medium.

The Record shall include clear descriptions of Personal Data types, Data Subject types, the business function and purpose for the processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

8. REPORTING A PERSONAL DATA BREACH

Data Protection Legislation requires us to notify any **Personal Data Breach** to the applicable Supervisory Authority and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected **Personal Data Breach** and will notify Data Subjects or any Supervisory Authority or other regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the **DPO** and **Senior Info/Cybersec Manager** in accordance with the company's Breach/Incident Management Procedure and preserve all evidence relating to the potential/actual **Personal Data Breach**.

9. AWARENESS & TRAINING AND AUDIT

You must undergo all mandatory data protection related training and ensure your team undergo similar training in accordance with the company's mandatory training policy.

You must regularly review all the systems, processes and procedures under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Williams & Wilson

Premier Business Centre, 10th Floor Sterling Tower, 14
Poudriere Street, Port Louis, Mauritius
Tel: +44 203 996 1492
E-mail:admin@williamsandwilson.org
Website: www.williamsandwilson.org