MasterIT

Privacy Policy

Author	SL Nossel
Version	V1.1

Version Control

Version	Date	Author	Summary of Changes
V0.1	27 March 2023	SL Nossel	Initial Draft, Data Governance and Third Party Services
V0.2	12 April 2023	SL Nossel	Amended Draft
V1.0	4 May 2023	SL Nossel	Finalised Data Protection and Privacy
V1.1	19 June 2023	SL Nossel	Amended Structure

Table of Contents

1 INTRODUCTION

Respecting and protecting your privacy and Personal Information is very important to MasterIT. It is also a Constitutional right and good business practice requirement which we take very seriously.

The Privacy Policy applies to you, the data subject, and governs the relationship with MasterIT.

For more detailed information with regards to the processing and protecting of your personal information please contact the MasterIT Information Officer as stipulated in section 10 below.

In line with the 8 Conditions for Lawful Procession of Personal Information as set out in the Protection of Personal Information Act no 4 of 2013 (the Act), we-

- Accept joint responsibility and accountability with you to responsibly manage and protect your Personal Information when providing our services and solutions to you;
- Undertake to collect and process only such Personal Information which is necessary given the purpose for which it is processed and to assist you with your required solutions, conclude the necessarily related agreements and consider the legitimate legal interests of everyone concerned, as required by the Act. We will at all times respect your right to withdraw your consent for the processing of your Personal Information;
- Undertake to only use your Personal Information for the purpose for which the information is essential to enable us to assist you or provide solutions to you;
- Undertake not to share or further process your Personal Information with anyone or for any reason if not required for assisting you with your solutions or as required in terms of legislation or regulations;
- Undertake to take reasonably practicable steps to ensure that information is complete, accurate, not misleading and, where necessary, is updated;
- Undertake to be open and transparent on the nature, extent and reasons for processing Personal Information;
- Undertake to safeguard and protect your Personal Information in our possession;
- Undertake to freely confirm what Personal Information we hold of you, to update and rectify the Personal Information upon request and to keep it for no longer than required.

By providing us with your Personal Information, you agree to this Policy and authorise MasterIT to process such information as set out herein and you authorise MasterIT and any associated entities or third parties (where applicable) for the purposes set out herein. We will not use your Personal Information for any other purpose than that set out in this Policy and we will take the necessary steps to secure the integrity and confidentiality of Personal Information in our possession and under our control by taking appropriate and reasonable measures to prevent loss of, damage to or unauthorised destruction of your Personal Information and to prevent the unlawful access to, or processing of Personal Information.

2 PURPOSE OF DATA COLLECTION

The MasterIT app collects and processes user data for the following purposes:

1. Rewarding Learners: The app aims to incentivize and reward learners for developing better learning habits. User data is utilized to track goal completion rates, achievements, and engagement levels, enabling the app to provide relevant rewards and incentives.
2. Driving Positive Learning Behaviours: By leveraging technology and behavioural economics, MasterIT encourages positive learning behaviours such as improved attendance and better engagement. User data is analysed to identify barriers and obstacles to optimal studying, allowing the app to provide tailored recommendations and interventions.
3. Providing Insights to Institutions: MasterIT generates valuable data insights for partnering institutions. This data, which is always anonymized to ensure privacy, offers institutions a comprehensive view of their learners' behaviours, including trends in engagement and studying behaviours. These insights enable institutions to make informed decisions, implement targeted interventions, and enhance the learning experience.
4. Limited Data Sharing with Universities: MasterIT shares limited and anonymized data with the universities it partners with. This data typically includes goal completion rates and trends in study behaviours. The purpose of sharing this data is to assist universities in evaluating the effectiveness of their educational programs, identifying areas for improvement, and enhancing overall learner outcomes.

It is important to note that all data shared with universities undergoes a rigorous anonymization process to ensure user privacy and compliance with applicable data protection regulations. MasterIT prioritizes the confidentiality and security of user data throughout all data sharing activities.

Additionally - MasterIT may, from time to time, collect and process data for any of the following purposes:

1. To confirm and verify your identity or to verify that you are an authorised user for security purposes.
2. To comply with all legislative or regulatory requirements related to services provided to you by us.
3. To comply with possible requirements by the Information Regulator or other Government agencies allowed by law, legal proceedings, or court rulings.
4. To respond to your queries or provide support.
5. To monitor platform usage, user engagement, service quality and performance.
6. To administer, manage, monitor and develop the app or platform.

3 DATA RESIDENCY

MasterIT maintains data infrastructure across the United States, the United Kingdom, the European Union as well as Australia. Dependent on your institution data may reside across any of these regions and may from time to time be shared across multiple regions for the purposes set out in this Privacy Policy. This will be done in very limited circumstances and in strict adherence of all requirements of the POPI Act, GDPR and other relevant legislation.

4 THIRD PARTY PROVIDERS/OPERATORS

We may need to share your Personal Information and/or utilise software or online platforms to enter and process your information for business management purposes. This will only be done in strict adherence to the requirements of the Act. We also have agreements in place to ensure that they comply with the privacy requirements as required by the Act.

The MasterIT app utilizes certain third-party services, such as Firebase Storage, Firestore Database, Google Analytics, Firebase Cloud Messaging, Firebase Authentication and Algolia Search. These services are chosen for their reliability, security, and privacy practices. User data may be processed and stored within these services as required for the app's functionalities.

When using Firebase, Google is generally a data processor under GDPR and processes personal data on our behalf. Similarly, when using Firebase, Google generally operates as a service provider under the CCPA handling personal information on our behalf. Firebase terms include Data Processing and Security Terms detailing these responsibilities.

Crashlytics and App Distribution are governed by the Firebase Crashlytics and Firebase App Distribution Terms of Service, and are covered by those associated data processing terms.

Google Analytics for Firebase and Google Analytics are governed by the Google Analytics for Firebase Terms of Service and the Google Analytics Terms of Service, respectively, as well as the Google Ads Data Processing Terms.

Algolia Search is governed by the Algolia Terms of Service and Privacy Policy.

MasterIT may also disclose your information:

1. Where we have a duty or a right to disclose in terms of legislation, regulations or industry codes;
2. Where we believe it is necessary to protect our rights;
3. When explicitly requested by you;
4. With professional advisers, for example, law firms, as necessary to establish, exercise or defend our legal rights and obtain advice in connection with the running of our business. Personal Information may be shared with these advisers as necessary in connection with the services they have been engaged to provide.
5. To law enforcement, regulatory and other government agencies and to professional bodies, as required by and/or in accordance with applicable law or regulation. We may also review and use your personal information to determine whether disclosure is required or permitted.

5 DATA SECURITY

At MasterIT, the security of user data is of utmost importance. We have implemented robust measures to safeguard user information and ensure its confidentiality and integrity. Here's an overview of our data security practices:

1. Encryption: We employ industry-standard encryption techniques to protect user data during transmission and storage. This includes the use of secure communication protocols (such as HTTPS) to encrypt data in transit, as well as encryption algorithms to protect data at rest.
2. Access Controls: Access to user data is strictly controlled and limited to authorized personnel who require access to perform their designated tasks. We follow the principle of least privilege, ensuring that access permissions are granted based on job roles and responsibilities.
3. Authentication and Authorization: User authentication is enforced to verify the identity of individuals accessing the app and its associated data. Strong authentication mechanisms, such as passwords or biometric authentication, are utilized to prevent unauthorized access. Role-based access control (RBAC) is implemented to assign specific privileges and access levels to authorized users.
4. Regular Security Assessments: We conduct regular security assessments, including vulnerability scanning and penetration testing, to identify and address any potential security weaknesses or vulnerabilities in our systems. These assessments help us proactively mitigate security risks and maintain a robust security posture.
5. Data Minimization: We follow the principle of data minimization, collecting only the necessary data required to provide the intended app functionalities. We do not retain personal data for longer than necessary and ensure appropriate data anonymization or deletion when it is no longer needed.
6. Data Backups and Disaster Recovery: Regular data backups are performed to ensure data integrity and availability. In the event of an unforeseen incident or data loss, we have disaster recovery measures in place to restore data and minimize any potential impact on user information.
7. Staff Training and Awareness: We prioritize staff training and awareness regarding data security practices. Our employees are educated about the importance of data protection, privacy regulations, and best practices for handling sensitive information.
8. Compliance with Regulations: We adhere to applicable data protection regulations and industry best practices. This includes compliance with laws such as the General Data Protection Regulation (GDPR) and Protection of Personal Information Act (POPI), where applicable, to ensure the privacy rights of our users are respected and protected.

While we take extensive measures to secure user data, it is important to note that no system or method of data transmission over the internet can be guaranteed to be 100% secure. In the event of any data breaches or security incidents, we have established incident response procedures to promptly address and mitigate the impact.

At MasterIT, maintaining the trust and privacy of our users is a top priority, and we are committed to continuously enhancing our data security practices to adapt to evolving threats and technologies.

6 DATA RETENTION

We shall only retain and store Personal Information for the period for which the data is required to serve its primary purpose or a legitimate interest or for the period required to comply with an applicable legal requirement, whichever is longer. Once data is no longer required, it is securely anonymized or deleted to further protect user privacy.

7 DATA ACCESS

You have the right to request a copy of the Personal Information we hold about you. To do this, simply contact us via the numbers/addresses provided below or on our website and specify what information you require. We will need proof of authorisation or a copy of your ID document to confirm your identity before providing details of your personal information.

Please note that any such access request may be subject to a payment of a legally allowable fee.

8 CONTACT US

If you have any queries about this policy, or need further information about our privacy practices, wish to withdraw consent, exercise preferences or access or correct your personal information, please contact us at: support@master-it.app

Any additional information or concerns can be found and raised with the Information Regulator, who can be contacted as shared below, but please feel free to contact us first to discuss any questions or concerns you may have -

Website: https://www.justice.gov.za/inforeg/

Tel: +27 12 406 4818

Email: inforeg@justice.gov.za

9 PERSONAL INFORMATION DEFINITION

Personal Information is defined by the Protection of Personal Information Act (the Act) as:

"information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
b. information relating to the education or the medical, financial, criminal or employment history of the person;
c. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
d. the biometric information of the person;
e. the personal opinions, views or preferences of the person;
f. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g. the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person".
h. Respecting and protecting your Personal Information (please refer to the definition of Personal Information at the end of this policy statement) is very important to us. It is also a Constitutional right, legal, and good business practice requirement, which we take very seriously.