1. Purpose and Scope:

The purpose of the ICT 15 App is to enable users to report emergency cases promptly to the ICT Police for immediate response and assistance. This policy governs the handling of data collected through the ICT 15 App and applies to all stakeholders involved in the data processing.

2. Data Collection and Minimization:

The ICT 15 App will collect only the necessary data required for emergency reporting and response. This includes the user's location, contact information, and details of the emergency situation. No additional personal data beyond what is essential for emergency response will be collected.

3. Data Security and Encryption:

Data transmitted through the ICT 15 App will be encrypted to protect it from unauthorized access during transmission. All data stored within the app and backend servers will also be encrypted to ensure its security.

4. Data Access and Authorization:

Access to data within the ICT 15 App will be restricted to authorized personnel with appropriate roles and permissions within the ICT Police. Users' personal data will be accessible only to the ICT Police officers and emergency responders who are directly involved in handling the reported cases.

5. Data Retention and Deletion:

Data collected through the ICT 15 App will be retained only for as long as necessary to handle the emergency case effectively. Once the emergency situation is resolved and the case is closed, personal data will be promptly deleted, adhering to relevant data retention laws and guidelines.

6. Informed Consent:

Users will be informed about the data collected, its purpose, and how it will be handled through the ICT 15 App. Explicit consent will be obtained from users before they submit their emergency reports.

7. Anonymization and Pseudonymization:

Where possible, personal data will be anonymized or pseudonymized to protect the identities of individuals in the emergency reports, especially when sharing aggregated data for statistical or analytical purposes.

8. Data Breach Response Plan:

A comprehensive data breach response plan will be in place to handle any potential data breaches through the ICT 15 App. This plan will include steps for immediate containment, notification to affected parties and authorities, and measures to prevent future breaches.

9. Data Subject Rights:

Users will have the right to access, correct, or delete their personal data stored within the ICT 15 App. Procedures will be in place to handle data subject requests in a timely and compliant manner.

10. Data Transfer and Sharing:

Data sharing with third-party services or organizations will be strictly limited to what is necessary for emergency response purposes and will be conducted in accordance with relevant laws and regulations.

11. Training and Awareness:

All personnel involved in handling data through the ICT 15 App will receive appropriate training on data handling policies, security protocols, and the importance of protecting user data.

12. Compliance and Auditing:

Regular audits will be conducted to ensure compliance with this data handling policy and relevant data protection laws. Any identified gaps or issues will be addressed promptly to maintain data security and privacy.

13. Public Transparency:

Information about the data handling practices of the ICT 15 App used for emergency reporting to the ICT Police will be made publicly available to instill trust among users and demonstrate the commitment to protecting their privacy.

This data handling policy will guide the responsible and secure management of data collected through the ICT 15 App for emergency reporting to the ICT Police, ensuring efficient emergency response while safeguarding user privacy and data security.