



Traffic Escort Wardens

Security & Privacy Overview

Version 1.0 • July 2026

This document provides a high-level overview of the security and privacy measures implemented within the Traffic Escort Wardens application. It is intended as an easy-to-read summary and should be read together with the application's published Terms of Service, Privacy Policy, Data Handling & Security Statement, Subscription Policy and other legal documents available through the subscription website.

1



User Authentication and Access Security

Access to the Traffic Escort Wardens application is restricted to authorised users. Users authenticate using their Google account through Google's secure identity platform. Passwords are never stored or managed by the application. Where Multi-Factor Authentication (MFA) is enabled on a user's Google account or enforced by their organisation, that additional protection is automatically applied during sign-in. Once authenticated, AppSheet row-level security ensures users can access only the work orders and records they have been authorised to view. Communication between users, AppSheet and supporting services is protected using HTTPS/TLS encryption.

2



Protection of Sensitive Personal Information

Sensitive personal information, including driver's licence numbers, is protected using application-level encryption before permanent storage. Licence numbers are retained in encrypted form within the application's database and are only decrypted within authorised backend processes when operationally required for secure exchange with authorised systems such as TESS. Where practical, only a masked version of the licence number is displayed to users.

3



Cloud Data Storage Security

Application data is hosted within Google's cloud-based AppSheet platform rather than on privately managed database servers. Google manages the underlying cloud infrastructure, physical data centre security, platform resilience and core platform security controls. Application-specific controls — including user permissions, row-level access, encryption workflows, validation and business rules — are implemented within the Traffic Escort Wardens application.

4



Layered Security Model

- ✓ Google-managed user authentication
- ✓ Multi-Factor Authentication where enabled on the user's Google account
- ✓ AppSheet row-level security restricting users to authorised records
- ✓ Application-level encryption of sensitive personal information
- ✓ HTTPS/TLS encryption protecting data in transit
- ✓ Google-managed cloud infrastructure supporting secure data hosting
- ✓ Server-side validation and controlled backend integrations
- ✓ Audit logging and policy acceptance records supporting accountability



This overview is a plain-English summary only. The full published legal documents remain the authoritative source for the terms governing use of the service.



Traffic Escort Wardens

Security & Privacy Overview

Version 1.0 • July 2026

5



Independent Operation

The Traffic Escort Wardens application is independently operated by Tim Elleston. It is designed to complement existing operational systems by providing a practical field-user interface, automation and workflow improvements. It is not represented as a Main Roads Western Australia product or as an officially endorsed application unless confirmed in writing.

6



Practical Security and Privacy Controls

Examples of controls that have been implemented within the service include:

- ✓ Authenticated Google accounts for controlled user sign-in.
- ✓ AppSheet row-level security to restrict each user to authorised records.
- ✓ Encrypted driver's licence numbers, with masked display where appropriate.
- ✓ Local audit logging to support traceability of important application activity.
- ✓ Policy acceptance records recording acceptance of the published terms and policies.
- ✓ Server-side validation for controlled processing and backend integrations.
- ✓ Stripe-hosted payment processing, so card details are handled through Stripe rather than stored by the Traffic Escort Wardens application.

7



Commitment to Security

The application has been designed to minimise the exposure of sensitive information while providing authorised users with the information required to perform their duties. Security and privacy controls will continue to be reviewed and improved as the application develops, operational requirements change and new risks are identified.



Important: This overview is a plain-English summary only. The full published legal documents remain the authoritative source for the terms governing use of the service.