Anti-Paste Guard — User Manual

Overview

Anti-Paste Guard is a desktop application designed to help instructors, exam proctors, and administrators ensure the authenticity of typed work by monitoring copy-paste activity and unusual text input behaviors. The system is privacy-conscious: it never records the actual text content, only event metadata (timing, counts, app focus). This allows reliable anomaly detection without exposing sensitive user data.

Getting Started

Launching the Application

1. Locate and open **AntiPasteGuard.exe** from the **dist/AntiPasteGuard/** folder (or use the provided installer).
2. The main window will appear, titled **Anti-Paste Guard**.
3. Click **Start Capture** to begin monitoring; the status bar will show *Capture: ON*.
4. Click **Stop Capture** to pause monitoring.

Main Window

Dashboard Components

- **Event Feed**: Displays real-time event summaries (keystrokes, paste events, anomalies).
- **Anomaly List**: Shows flagged behaviors with severity levels (HIGH, MEDIUM).
- **Metrics Panel**: Displays words per minute (WPM), characters per minute (CPM), and typing delay averages.
- **Chart Panel**: Timeline view of typing activity and anomalies.
- **Export Button**: Save event/anomaly data to CSV for review or audit.

Interpreting Anomalies

- **Idle-to-Burst (HIGH)**: Long pause followed by sudden large paste — suggests copy-paste.
- **Multi-Paste Streak (MEDIUM)**: Several pastes close together — suspicious repeated usage.
- **Text Injection (HIGH)**: Large text appears without corresponding keystrokes — possible AI/macro input.
- **Uniform Typing (MEDIUM)**: Extremely regular typing intervals — automation suspected.

Verifying Logs

Anti-Paste Guard stores events in a tamper-evident encrypted log. To verify logs:

1. In the dashboard, click **Verify Database**.
2. A report will open showing if all records are valid and untampered.
3. “OK” indicates verification success. Any failures will list errors and suggested fixes.

Security Notes

- Logs are encrypted and signed to prevent tampering.
- Clipboard monitoring only records metadata (length/type), never actual clipboard content.
- The application works offline; no cloud connection is required.

Best Practices

- Start the app before distributing exams or assignments.
- Run verification at the end of the session.
- Export CSV logs for record keeping.
- For sensitive environments, keep the master key file secure.

Troubleshooting

- **Dashboard not opening**: Use the packaged .exe or ensure Python/Tkinter runtime is available.
- **Metrics not updating**: Ensure capture is started (Start Capture).
- **Verification errors**: Try re-running verification; errors may indicate improper shutdown or missing master key.