Graftcode Toolkit — Privacy Policy

Product	Graftcode Toolkit, a Chrome DevTools extension.
Controller	Graftcode S.A., Franciszka Klimczaka 1, 02-797 Warsaw, Poland.
Contact	privacy@graftcode.com
Site	https://graftcode.com/
Last updated	29 October 2026

This policy describes what the extension reads, what it stores on the device, and what it does not send anywhere. It covers the extension only. The Graftcode website has its own privacy policy.

What the extension does

Graftcode Toolkit adds a **Graftcode** panel to Chrome DevTools. When you turn **Capture** on for the tab you are inspecting, the extension decodes Hypertube WebSocket traffic from that page and shows the call trace in DevTools.

Capture is off when you install the extension. It applies only to the inspected tab, turns off when you close DevTools for that tab, and is not restored after the browser restarts. A reload of that same tab can keep Capture on only until DevTools closes.

There is no toolbar button. Links in the panel (Graftcode, Docs, Discord) open only when you click them. Those clicks do not attach captured frames, headers, or payloads.

Where it runs

The extension's script is present on every `http` and `https` page, including a site on your own domain that uses Graftcode. It does not read the page until you turn Capture on for that tab.

Data processed while Capture is on

Only while Capture is on for that tab, and only in that tab, the extension reads:

- **Website content.** Binary WebSocket frames on that tab whose path contains `/graft-ws/`, or whose path is `/ws`, on any host. Frames are decoded in the browser into a call trace, request and response previews, and related session, assembly, and plugin views. Call bodies are shown in full, because that is the debugging feature. They can contain whatever the application put in the call. Other socket paths are ignored.
- **Authentication information.** Session and GraftConfig header values. A header whose name matches token, authorization, cookie, secret, password, JWT, or bearer is redacted before display. Values of eight characters or fewer become `***`. Longer values keep the first four and last four characters, plus the length. Other header names are shown as received. Lines in a connection string that start with `licensekey` are dropped and not shown.
- **Configuration.** GraftConfig name, runtime, host, modules, and channel, so the panel can label the socket.

This processing stays in memory: the page hook, the extension service worker, and the DevTools panel. It is dropped when you close DevTools for that tab or when the browser restarts. Call bodies are not written to disk.

What is stored

- **`chrome.storage.local`**, key `gcDebugTraceLayout`: panel layout only. That is theme, column widths and order, splitter position, whether the inspector is visible, JSON line wrapping, and preview mode. It does not contain page content, frames, headers, or payloads. On startup the extension also deletes a legacy `captureEnabled` key if one is present. Capture itself is not saved in `chrome.storage`.
- **`sessionStorage` on the page**, key `graftcode-gc-debug/capture`: the single value `1` while Capture is on for that origin, so the hook can arm before the page opens its socket. The extension removes the key when Capture turns off. The key does not hold frames or payloads.

What is not sent

The extension does not:

- send frames, headers, payloads, or config to Graftcode or to any other server
- use analytics, advertising, cookies, or remote code
- sell or transfer user data
- use data for credit, lending, or any purpose other than showing the debug trace to the person who turned Capture on

Permissions

The only extension permission is `storage`, for the layout preferences above. The extension does not request browsing history, and it does not request access to all websites.

Contact

Questions about this policy: privacy@graftcode.com.
