WoW Portal and Child App Security

> **Important:** The WoW Portal and Child Apps comprise a substantial codebase exceeding 100,000 lines, entirely generated through AI-driven development. The Child Apps leverage multiple AIs in complex combinations and sequences. An extremely complicated digital ecosystem that is not yet fully understood or controlled. Consequently, this documentation may contain inaccuracies or omissions that could negatively impact your security. However, we have done everything in our power to give you control over and protect your data so that you can harness the power of AI as securely and effectively as possible.

1. What WoW Portal and Child Apps are

- The WoW Portal is where you sign in, hold your shared credit balance, buy credits, redeem coupons, and launch Child Apps.
- The Child Apps are separate tools (e.g., WoW Factor Generator) that the WoW Portal launches for you. They run only in your browser—they have no database of their own. Anything you type or generate in a Child App exists only temporarily in your browser tab and is lost when you close the tab and clear your browser data.
- When you launch an app, we load it inside a sandboxed iframe in your browser. The browser sandbox is a hard isolation boundary—the app cannot read your files, access other tabs, install software, or touch your operating system.
- The only thing Child Apps may see from your session, and that is stored in the portal, is an error code if the app crashes or generates an error report. For more information, see the section "3. Crash and error reporting" below.
- To store your data, use the app's export options and save it locally on your computer.
- Both the WoW Portal and the Child Apps were built on Lovable and have passed Lovable's automated security scans. We build every app in the WoW Portal on the Lovable platform (React + Supabase + edge functions) and pass automated security scans for exposed secrets, missing access controls, and known-vulnerable dependencies before it goes live.
- In the Lovable AI dashboard, content logging of AI communication is disabled. Portal admins see and retain only summary metrics (model, tokens, duration, cost) for your AI calls.
- We handle login through Supabase Auth, which issues short-lived JWT (JSON Web Token) sessions. For app launches, we generate single-use tokens with 244 bits of entropy— so even a leaked launch URL can't be reused.
- All communication between your browser and the WoW Portal and all Child Apps is encrypted over https://
- Anyone with admin privileges on the WoW Portal must verify on every new device using an authenticator app (Google Authenticator, 1Password, etc.) Trusted devices are remembered for 30 days, then re-verified. This protects the platform—and you.
- We give you full transparency on credits. You top up once and use the credits across all Child Apps. Every transaction is logged, and you can download a printable receipt at any time from your Payments page.
- All payments go through Stripe, which handles your card details.

- We make GDPR deletion truly one-click. Click "Delete account," re-enter your password, and we will permanently remove your account and all related data via a server-side cascade. No soft-delete, no leftovers, no follow-up emails required.

> **Important:** We advise you to anonymize all information and data before uploading or entering it. Remove names of people, companies, brand names, and other identifying details wherever possible.

2. What is actually stored, and where

Data	Where it lives	Who can see
Your email, password (hashed), and login sessions.	Portal backend (Lovable Cloud).	Only you and the portal admin (not the password).
Your credit balance, payment history, and coupon redemptions.	Portal backend.	Only you and the portal admin.
Anything you upload, type, or generate inside a Child App.	In your browser and is transmitted to and analysed by an external third-party AI service.	Only you and the third-party AI service can see your data, information and content. Portal is configured to see and retains summary metrics of AI requests (model, tokens, duration, cost). AI models are not secure storage solutions, and users are advised be cautious when sharing sensitive information.
Stripe payment details (card numbers, etc.)	Stripe — data never touches the WoW Portal	Only Stripe and you.
Error codes if the app crashes or an error toast is issued.	Your browser tab plus the error code that is sent and stored in the Portal backend.	Admin can see the error code the Child App issued. For example, "WF-ACCOUNT-DELETE-FAIL". For more information, see section 3.

> **Important:** Child Apps do not store your work. If you need to keep something a Child App produced, you must save or export it yourself before closing the tab and storing it on your local computer.

3. Crash and error reporting

Both the WoW Portal and the Child Apps can let us know if they experience an error or crash when you run them. If you encounter an error or crash, the app sends a simple, pre-approved error alert to the WoW Portal. This error message is a standardized text and has nothing to do with the content in your browser or your personal data.

The sole purpose is to identify and resolve problems or bugs and improve the app's stability and performance.

What we collect and send back:

- The app identifier name, always a two- or three-letter code like "WP"
- The pre-registered error code, typically something like "ACCOUNT-DELETE-FAIL"
- The severity level assigned to that code
- A timestamp and a resolved/not-resolved flag, for internal follow-up
- Only codes registered are accepted. We reject any unknown or malformed request.

What we never collect and send back:

- Error messages, stack traces, or line numbers
- URLs, page paths, or route history
- User IDs, names, email addresses, or account details
- IP addresses, browser fingerprints, device information, or user agents
- Any content, files, or data processed inside the app

4. Security at WoW Portal (backend)

Section 4 only describes the WoW Portal, not Child Apps.

Authentication & Access Control

- All user accounts are protected by email-and-password authentication with mandatory email verification — you must confirm your email address before you can sign in. Passwords are never stored in plain text; they are hashed using industry-standard algorithms managed by our authentication infrastructure.

Data Isolation with Row-Level Security

- Every database table is protected by Row-Level Security (RLS) policies enforced at the database level to increase protection for user profiles, payments, invoices, and credits.

Role-Based Access

- Administrative functions are protected by a dedicated roles system stored in a separate, secured table. Admin privileges are verified server-side using security-defined functions.

Secure Payments

- Credit purchases are processed entirely through Stripe, a PCI DSS Level 1 certified payment processor. You enter your card details directly on Stripe's hosted checkout page—they never touch our servers. Payment verification and credit fulfillment occur server-side via secure backend functions.

Secure Backend Architecture

- All sensitive server-side logic (payment verification, coupon redemption, app launching) runs in isolated backend functions with dedicated service-role access. Client-side code communicates only through authenticated API calls with JWT tokens.

Infrastructure

- The platform runs on Lovable Cloud, built on enterprise-grade open-source infrastructure (Supabase/PostgreSQL) with encrypted connections (TLS/SSL) for all data in transit.

5. To the best of our knowledge

1. Portal account risk — low, but real
   - If someone gets your Portal password, they can sign in as you, spend your credits, and see your email address and purchases. They cannot see your card details (which are stored live with Stripe), but they can drain your balance.
   - Mitigation already in place: strong password checks, optional multi-factor authentication for admins, and a mandatory legal disclaimer.
   - What users should do: use a unique, strong password and don't share it.
   - The data you enter in Child Apps lives in your browser and is shared with third-party AIs. We do not offer any databases to store your data. You have to store your data on your local computer. So even if someone gets your password or hacks the portal, they cannot see your data in the Child Apps.

2. Losing your work in Child Apps — medium likelihood, low severity
   - Because Child Apps store nothing server-side, closing the tab, refreshing, or a browser crash will erase whatever you were working on.
   - What users should do: download or export results before closing the tab using the options offered in the Child Apps. Treat Child Apps like a whiteboard, not a filing cabinet. A whiteboard that is cleaned after you close your browser. A whiteboard that is also cleaned if your browser crashes. Therefore, as with all other computer programs or apps, make it a habit to export and store your data and results frequently on your local computer.

3. Shared-device risk — low, but worth mentioning
   - If you sign in on a shared or public computer and walk away without signing out and clearing browser data, the next person could use your account and access your data, including using your credits.
   - What users should do: always sign out on shared devices, clear browser data, and avoid using the WoW Portal on computers you don't control.

4. Browser/extension risk — low
   - Malicious browser extensions can read anything you see on a web page. This applies to any website, not just the WoW Portal.
   - What users should do: only install browser extensions you trust.

5. Phishing risk — low, but always present
   - Someone could send a fake "Portal login" email to trick you into entering your password on a fake site.

- What users should do: only sign in directly to the WoW Portal address yourself, and verify the URL in the address bar before entering your password.

6. Child Apps cannot reach into the WoW Portal — by design
   - Child Apps run in sandboxed frames and use single-use, lived launch tokens. A Child App cannot read your email, your password, your credit balance details, or anything from another Child App.

7. Data leakage through the AI – risk unknown, but real
   - The third-party AI services used by Child Apps may not store your data permanently; however, there is still a risk of unintended exposure or misuse of your data and information during processing and analysis. Furthermore, once the data leaves your browser, you have limited control over how it is handled, which could violate data protection regulations or compromise sensitive information. We advise you to anonymize all information and data before uploading or entering it. Remove names of people, companies, brand names, and other identifying details wherever possible.

7. It's worth being transparent.

Lovable's automated security scan checks for common issues (database access rules, leaked keys, missing authentication, common privilege-escalation patterns). Passing it means none of those common issues were found—it is not the same as a full professional penetration test; for most small-to-medium use cases, that's appropriate. This is a demo site for educational and training purposes. If you run sensitive data in any Child App, you do so at your own risk. We advise you to anonymize all information and data before uploading or entering it. Remove names of people, companies, brand names, and other identifying details wherever possible.

8. DISCLAIMER & LIMITATION OF LIABILITY (SWEDEN)

Below is our Disclaimer & Limitation of Liability, which must be accepted during login, dated 260803. What you accepted during login might be different. We have the right to change the Disclaimer & Limitation of Liability at any time. It is your responsibility to download and save the Disclaimer @ Limitation of Liability at login and before acceptance. On our homepage www.creating-wow-products.com you can also view and download our **Terms of Use and Sale & Conditions**, which also apply to your use of the portal and all Child Apps.

Applicability: The following terms apply to your access and use of this portal and all applications, tools, and services provided within it (collectively, the "Apps"). By accessing or using the Apps, you explicitly agree to these terms.

1. No Professional Advice & Assumption of Risk
The Apps and any output generated by them are provided for general informational, experimental, and educational purposes only. They do not constitute legal, financial, technical, or other professional advice. You agree that you use the Apps and rely on any generated results entirely at your own risk. Any decisions made based on the Apps' output are solely your responsibility.

2. "As Is" and "As Available" Disclaimer
The Apps are provided on an "AS IS" and "AS AVAILABLE" basis. To the fullest extent permitted by applicable law, we expressly disclaim all warranties of any kind, whether express, implied, or statutory, including but not limited to warranties of merchantability, fitness for a particular purpose, non-infringement, and continuous, error-free, or secure operation. We do not guarantee the accuracy, completeness, or reliability of any results.

3. Third-Party Services and AI Dependencies
The Apps may utilize external third-party services, APIs, and artificial intelligence (AI) programs. We have no control over these third-party services. We are not responsible for their availability, accuracy, data handling, or any errors, omissions, or "hallucinations" (false information) generated by underlying AI models. Your use of third-party integrated services is at your own risk.

4. Limitation of Liability
To the maximum extent permitted by applicable law, we (and our affiliates, developers, and partners) shall not be liable for any direct, indirect, incidental, special, consequential, or punitive damages. This includes, but is not limited to, loss of profits, loss of revenue, loss of data, business interruption, or loss of goodwill arising out of or in connection with your use, or inability to use, the Apps or the portal.

Our total, aggregate liability to you under any circumstances, regardless of the cause of action, shall be strictly limited to the amount you paid to us to use the Apps in the past four (4) weeks, or SEK 100 (One Swedish Krona), whichever is greater.

5. Indemnification
You agree to indemnify, defend, and hold us harmless from any claims, liabilities, damages, losses, and expenses (including reasonable legal fees) arising out of or connected with your misuse of the Apps, your violation of these terms, or your violation of any third-party rights.

6. Mandatory Legal Exceptions
Nothing in this disclaimer shall limit or exclude our liability for death or personal injury caused by our negligence, for fraud or fraudulent misrepresentation, or for any other liability or damages that cannot be lawfully limited or excluded under applicable Swedish law (such as intentional misconduct or gross negligence). If you are using the Apps as a consumer, certain statutory consumer rights may apply that cannot be altered by this agreement.

7. Governing Law and Dispute Resolution
These terms and your use of the Apps shall be governed by and construed in accordance with the substantive laws of Sweden, without regard to its conflict of law principles. Any dispute, controversy, or claim arising out of or in connection with this disclaimer or the use of the Apps shall be settled exclusively by the Swedish public courts, with the Stockholm District Court (Stockholms tingsrätt) as the court of first instance. No arbitration shall apply. All proceedings and documentation shall be conducted in Swedish.