



# AI Context Guard

**Protect your data from accidental leaks on ChatGPT, Claude, Gemini, and other AI platforms.**

AI Context Guard is a browser extension that detects and warns you before you paste sensitive data (API keys, passwords, personal information, source code) into AI chat interfaces.



## Key Features



### Real-Time Detection

- Detects **40+ types of sensitive data** including:
  - API keys and tokens (AWS, GitHub, Slack, Stripe)
  - Private keys and passwords
  - Personally identifiable information (PII)
  - Protected health information (PHI)
  - Financial data (credit cards, IBAN)
  - Internal URLs and IP addresses
  - Source code patterns



### Smart Warnings

- Shows a clear warning before you leak data
- Displays severity level and types of sensitive data detected
- Gives you 3 options:
  - **Auto-Redact & Paste** - Automatically remove sensitive data and paste clean text
  - **Cancel** - Stop and clear the text
  - **Continue Anyway** - Proceed at your own risk (logs for audit)



### Privacy First

- **No cloud processing** - All detection happens locally in your browser
- **No data collection** - We don't send your text anywhere
- **No tracking** - No analytics or telemetry
- **GDPR compliant** - Your data never leaves your computer






## **Activity Dashboard**

- Real-time stats on today's activity
- See how many data leaks were prevented
- View recent detection events
- Clear history anytime

## **Customizable Settings**

- Enable/disable warnings
- Control auto-redaction behavior
- Adjust scan sensitivity
- Maintain audit logs for compliance

## **Supported Platforms**

-  ChatGPT (chat.openai.com)
-  Claude (claude.ai)
-  Google Gemini (gemini.google.com)
-  Microsoft Copilot (copilot.microsoft.com)
-  Google Bard (bard.google.com)

## **Installation**

### **From Chrome Web Store**

1. Visit [https://chrome.google.com/webstore/detail/ai-context-guard/\[ID\]](https://chrome.google.com/webstore/detail/ai-context-guard/[ID])
2. Click "Add to Chrome"
3. Click "Add extension"
4. Extension appears in your toolbar

### **For Developers / Self-Installation**

1. Download the extension files
2. Open `chrome://extensions`
3. Enable "Developer mode" (top right)

4. Click "Load unpacked"
5. Select the extension folder
6. Done!

## **How to Use**

### **Basic Usage**

1. Visit ChatGPT, Claude, Gemini, or Copilot
2. Paste text containing sensitive data
3. AI Context Guard detects it and shows a warning
4. Choose: **Auto-Redact**, **Cancel**, or **Continue**

### **Example: Pasting Code with Secrets**

```
# Database config
DATABASE_URL=mongodb://user:password123@prod.db.com
API_KEY=sk_live_51abc123def456
SECRET_TOKEN=ghp_ABC123XYZ789...
```

### **AI Context Guard will:**

- Detect 3 CRITICAL items
- Show a red warning dialog
- Offer to auto-redact and paste clean version:

```
# Database config
DATABASE_URL=[REDACTED]
API_KEY=[REDACTED]
SECRET_TOKEN=[REDACTED]
```

### **Checking Your Dashboard**

1. Click the extension icon in your toolbar
2. View today's stats:
  - Critical blocks prevented
  - High-risk items detected

- Auto-redacted events

3. Scroll down to see recent events

## **Adjusting Settings**

1. Right-click extension icon → "Options"

2. Toggle features on/off:

- Enable warnings (recommended: ON)
- Allow auto-redact (recommended: ON)
- Event logging for audit trail

3. Adjust scan delay for performance

4. View all detection types

## **Detection Capabilities**

### **CRITICAL Risk (Always blocks)**

- AWS API credentials
- Private SSH/RSA keys
- GitHub tokens
- Slack tokens
- Stripe API keys
- Database credentials
- Social security numbers
- Credit card numbers

### **HIGH Risk (Usually blocks)**

- API keys and bearer tokens
- Hardcoded secrets in code
- Internal IP addresses
- Medical record IDs
- Passport/driver license

- Internal domain names

### **MEDIUM Risk (Optional)**

- Email addresses
- Phone numbers
- Public URLs



### **Troubleshooting**

#### **Warning appears for every paste**

- This is normal for legitimate data paste operations
- Click "Continue Anyway" if the data is safe
- Or use auto-redact if you want clean text

#### **Extension not working on a website**

- Make sure it's one of the supported AI platforms
- Refresh the page (Ctrl+Shift+R)
- Check that extension is enabled in settings

#### **Too many false positives**

- Adjust scan delay in settings for better accuracy
- Report patterns that frequently trigger false alarms

#### **Performance issues**

- Increase scan delay in settings (default: 300ms)
- This reduces CPU usage during typing



### **Security & Privacy**

#### **What We Don't Do**

- **✗** We don't send your text to servers
- **✗** We don't track what you type
- **✗** We don't sell your data
- **✗** We don't use cookies for tracking

- ❌ We don't modify your clipboard permanently

## What We Do

- ✅ Scan text locally in your browser
- ✅ Log detection events locally (you can clear anytime)
- ✅ Store settings in your browser
- ✅ Show warnings to prevent data leaks

## Data Handling

All detection and processing happens **100% in your browser**. No data is sent to us or any third-party servers. You have full control and can clear history anytime.

## For Enterprises

### Team Deployment

- Deploy via Chrome Enterprise policies
- Enforce settings across organization
- Centralized event logging (with premium tier)
- Integration with security tools

### Compliance

- GDPR compliant (no data collection)
- SOC 2 audit-ready
- Generates audit logs
- Works with security frameworks

### Contact Sales

Email: [enterprise@example.com](mailto:enterprise@example.com) for:

- Volume licensing
- Custom integrations
- Dedicated support
- SLA guarantees

## **Report Bugs**

Found an issue? Help us improve:

1. Go to extension menu → "Report issue"
2. Include:
  - What you were doing
  - What happened
  - Browser and OS version
3. Submit

## **Feature Requests**

Want a new feature?

- Open Options → "Send feedback"
- Or email: [feedback@example.com](mailto:feedback@example.com)
- Top requests might be prioritized

## **Legal**

- **Privacy Policy:** [View full policy](#)
- **Terms of Service:** [View terms](#)
- **License:** [MIT License](#)

## **FAQ**

**Q: Will this slow down my browser?** A: No. Detection happens in the background with minimal CPU impact. Average scan time is <1ms.

**Q: Can I trust this with my real data?** A: Yes. Everything happens locally. We have no servers, no backend, and no way to see your data.

**Q: Does this work on mobile?** A: Not yet. Mobile Chrome doesn't support extensions yet, but we're working on browser extension equivalents.

**Q: What if I accidentally paste something anyway?** A: You have the full text in memory and can undo it on the AI platform (Cmd+Z or Ctrl+Z).

**Q: Can I turn this off?** A: Yes. Disable it in extension settings or remove it from Chrome anytime.





**Q: Will this work with future AI platforms?** A: We continuously add support for new platforms. Submit requests on our feedback page.

## Version History


### v1.0.0 (Current)

- Initial launch
- 40+ pattern detection types
- Auto-redaction
- Activity dashboard
- Full settings customization

## Support

-  Email: [support@example.com](mailto:support@example.com)
-  Bug reports: [GitHub Issues](#)
-  Community: [Discord](#)
-  Docs: [Full documentation](#)

---

Made with  to protect your data

AI Context Guard • © 2025 • [Website](#) • [Twitter](#)