UtterIDE Beta Disclaimer

Beta Status

UtterIDE is currently provided as a beta product.

The software may contain bugs, incomplete features, inaccurate AI outputs, unstable agent behavior, and unexpected side effects. Users should not rely on UtterIDE as their sole method for writing, reviewing, testing, deploying, migrating, or securing software systems.

UtterIDE is provided **“as is”** and **“as available”**, without warranties of any kind, whether express or implied.

Autonomous Agent Warning

UtterIDE is an autonomous review-first coding assistant integrated into Visual Studio Code.

Depending on enabled features and user permissions, UtterIDE may be able to:

- read files in the current workspace
- propose code changes
- create or modify files
- execute local terminal commands
- run tests or build commands
- interact with Git
- connect to configured databases
- generate SQL queries or migrations
- call third-party LLM APIs selected by the user

UtterIDE runs actions with the permissions available to the user’s local VS Code session and operating system account.

Users are responsible for reviewing all actions before approval.

Review-First Principle

UtterIDE is designed to be review-first.

Where supported, code changes should be shown as diffs before being applied. Users should review all proposed changes carefully before approving them.

Approval of a proposed change, command, Git action, database action, or migration means the user accepts the risk of that action.

Users should use Git, backups, sandboxed environments, Docker containers, test databases, and non-production environments whenever possible.

No Guarantee of Correctness

AI-generated code, SQL, commands, explanations, diagrams, migrations, and recommendations may be incomplete, insecure, outdated, destructive, or incorrect.

UtterIDE may misunderstand project structure, fail to detect edge cases, generate broken code, introduce security vulnerabilities, or execute an unsafe action if approved by the user.

Users are responsible for testing, reviewing, validating, and securing all outputs.

Terminal, Git and Database Risk

UtterIDE may support terminal, Git and database actions.

These actions can be dangerous.

Examples of possible harm include:

- data loss
- broken builds
- deleted files
- failed deployments
- corrupted repositories
- accidental commits or pushes
- modified databases
- dropped tables
- failed migrations
- production outages
- exposure of sensitive data

Users should not connect production systems unless they fully understand and accept the risk.

Production database actions, destructive commands, migrations, and Git pushes should always be reviewed with extra care.

Local Storage

UtterIDE does not require users to create an UtterIDE account.

UtterIDE does not operate a central backend server for storing user projects, prompts, code, database credentials, memory files, logs, or API keys.

UtterIDE stores project-related data locally, including files such as:

- `.utteride/memory.json`
- `.utteride/architecture.json`
- `.utteride/pii_rules.json`
- `.utteride/runs/`
- other local workspace metadata

Users are responsible for protecting, backing up, deleting, encrypting, or excluding these files from Git or other sharing systems where appropriate.

Local files may contain sensitive project information.

API Keys and Third-Party Providers

UtterIDE uses a Bring Your Own Key model.

Users may connect their own API keys for providers such as DeepSeek, Anthropic, OpenAI, Google, or other supported providers.

API keys are intended to be stored using Visual Studio Code's secure secret storage mechanisms where supported.

UtterIDE is not affiliated with DeepSeek, Anthropic, OpenAI, Google, Microsoft, or any other third-party provider unless explicitly stated.

Users are responsible for:

- obtaining valid API keys
- managing provider billing
- monitoring token usage
- complying with provider terms
- understanding where data is sent
- understanding provider retention and privacy policies

When a cloud LLM provider is used, selected prompts, code context, file content, database query results, or other workspace information may be sent from the user's machine directly to that provider.

Sensitive Data and PII Masking

UtterIDE may include local masking features designed to reduce the risk of sending sensitive data to third-party AI providers.

For example, database query results may be intercepted and masked based on rules defined in `.utteride/pii_rules.json`.

However, masking is not guaranteed to detect or remove all sensitive information.

Users are responsible for reviewing what data may be sent to third-party providers and for ensuring compliance with applicable privacy, confidentiality, employment, customer, contractual, and data protection obligations.

Users should not send secrets, passwords, API keys, private keys, customer records, personal data, health data, financial data, trade secrets, or production database records to cloud providers unless they are authorized to do so and understand the risks.

GDPR and Data Protection

Users are responsible for determining whether their use of UtterIDE involves personal data and whether they are acting as a data controller, processor, or in another legal role.

UtterIDE does not provide legal advice and does not guarantee compliance with GDPR, the EU AI Act, data protection law, employment law, cybersecurity law, sector-specific regulation, or contractual confidentiality obligations.

Organizations should review their own policies and consult qualified legal or compliance professionals before using UtterIDE with personal data, regulated data, customer data, production systems, or confidential business information.

No Professional Advice

UtterIDE may generate technical, security, database, architecture, compliance, or operational suggestions.

These outputs are not professional legal, security, financial, compliance, database administration, or engineering advice.

Users remain responsible for all technical and business decisions.

Pricing and Future Paid Plans

UtterIDE may be offered for free during beta.

Future versions may introduce paid plans, monthly subscription fees, premium features, commercial licensing, usage-based features, or supporter tiers.

Any future pricing will be communicated separately.

Third-party LLM usage, such as DeepSeek, Anthropic, OpenAI, Google, or other API usage, is separate from any UtterIDE subscription unless explicitly stated.

Users remain responsible for any costs charged by their chosen LLM providers.

Limitation of Liability

To the maximum extent permitted by applicable law, the developers and distributors of UtterIDE are not liable for any direct, indirect, incidental, consequential, special, punitive, or exemplary damages arising from use of the software.

This includes, but is not limited to:

- data loss
- code loss
- database loss
- security incidents
- downtime
- failed deployments
- broken builds
- API costs
- loss of business
- loss of profits
- unauthorized disclosure of information
- actions approved by the user
- third-party provider behavior

Some jurisdictions do not allow certain warranty exclusions or liability limitations, so some limitations may not apply.

User Responsibility

By using UtterIDE, the user acknowledges that:

- AI outputs can be wrong
- autonomous tools can be risky
- approved actions may modify local files, repositories, systems, or databases
- cloud LLM providers may receive selected context
- local project metadata may contain sensitive information
- backups, Git, sandboxing, and review are strongly recommended
- the user remains responsible for all actions performed through UtterIDE

If you do not accept these risks, do not use UtterIDE with important files, production systems, confidential data, regulated data, or live databases.