SECTION 01 / 10

Scope, operator and quick overview

What this policy covers

This Privacy Policy describes FixHubLab at fixhublab.com, its free browser tools, published blog, contact inquiries, optional Google Analytics and the owner-only administration area. It covers file processing on your device, saved preferences, website requests, inquiry handling and Google reports accessed by the operator. Another organisation has its own policy when you follow an external link. Read this policy with the Cookies page and Terms and Conditions.

Who is responsible

Fix Hub Lab operates the FixHubLab website at fixhublab.com. For support, privacy enquiries and requests about information held by the operator, email info@fixhublab.com. Fix Hub Lab is the business name provided by the operator; this policy does not claim a particular incorporated-company status, registration number or business address. The operator is responsible for information it determines how and why to use, such as support enquiries and relevant website records.

The short version

Public tools do not require an account. Selected tool images and PDFs, text, invoice details and calculator values are processed on your device and are not uploaded to the application server. Contact forms send the details you enter to Fix Hub Lab for inquiry handling. If the operator configures Google Analytics, its tag loads only after you opt into analytics. Ordinary website requests can generate hosting logs. The separate administration area requires owner authentication. The reasoning quiz keeps answers and raw practice scores in the page; it does not collect age or provide a clinical IQ assessment. Internet speed testing is an exception to local-only processing: its separate notice explains direct Cloudflare test traffic and data use.

Choices and limitations

Saved favourites and a remembered theme are optional. You can continue using the tools without enabling preference storage, change your choice through Cookie settings, and delete downloaded files using your device controls. Local processing does not guarantee that a shared computer, compromised browser or installed extension cannot access your information. Do not put confidential data in a URL or support message unless it is necessary.

Status of this document

Updated on 11 November 2026 for the current tool collection. The business name is Fix Hub Lab and the contact email is info@fixhublab.com. This remains an operator-review draft because hosting region, log and backup retention, email-provider arrangements and any applicable regional requirements still need confirmation. Document length is not a certification that every privacy law applies to, or has been satisfied by, this service.

SECTION 02 / 10

Information handled by the tools

Images and image metadata

The image compressor, resizer and converter read the file you select so your browser can decode pixels, show a preview and create a new image. The page may display the filename, file size, width and height. These details remain in the page rather than being submitted to a file-processing API. Image exports are produced from a browser canvas; do not rely on that process as a guaranteed removal service for every kind of metadata or hidden information.

PDF documents

The PDF merge and extraction tools read selected document bytes in browser memory. They inspect page counts and copy the pages you request into an output document. A PDF can contain names, signatures, embedded material, annotations or other personal information. Processing is local, but local processing does not make the document anonymous. Password-protected documents are not supported in this release; the tools do not attempt to bypass document encryption.

Text, JSON and calculations

The word counter, case converter and JSON formatter work with text entered in the workspace. Percentage, loan and profit calculators use the numeric values entered to compute a result. These tools do not create a user account, maintain a cloud history or send your text or figures to an AI service. JSON may contain credentials or personal records; avoid pasting live secrets even when using a local tool.

Invoice information

The invoice generator can process business and customer names, addresses, invoice references, line items, prices, taxes, due dates and notes. You choose what to enter. Invoice inputs and previews are not saved in a FixHubLab customer database. The download and print functions create a document on your device. Check that you have a proper reason and permission to use another person's details in an invoice.

What is not requested

The current tools do not request passwords, payment card numbers, identity documents, health information, precise location, camera access or microphone access. A document you voluntarily select may contain such information, so the responsibility to choose an appropriate file still matters. No payment processing, login account or paid subscription is provided by this release.

SECTION 03 / 10

Website requests, logs and communication

Basic connection information

When you request a page or asset, the web server and infrastructure receive the information needed to deliver it. Depending on hosting configuration, this can include your IP address, requested path, time, response status, browser user agent and referring page. Transport and security systems may also process connection and error details. These website records are different from the contents of a file selected inside a tool.

What the application does

The Node.js application serves the site, stores blog posts, uploaded blog images, site settings and contact inquiries in private application storage, and operates an authenticated administration panel. It does not keep a cloud history of visitor tool inputs. The operator can optionally connect read-only Google Search Console and Analytics reports. Avoid putting private information in URLs because requested paths can appear in browser history and infrastructure logs.

Enquiries you choose to send

The contact form sends your name, email address, subject and message to the website server after you acknowledge the privacy notice. The operator can read your message, change its handling status and add internal notes in the admin inbox. You can instead email info@fixhublab.com, in which case the email providers also process your correspondence. Tool processing and inquiry submission are different data flows; please send fictional or redacted examples rather than sensitive source files.

Contact page behaviour

The Contact us page displays the published business contact and a working inquiry form. Submitting the form stores the message in the private application database; it does not automatically email the operator. A separate email link opens your email application for you to review and send a message. Basic anti-spam measures include a honeypot, a signed form timestamp and request-rate limits. The default inquiry retention period is 180 days and can be changed by the operator.

Accuracy and necessary detail

Provide only information relevant to your enquiry. For a technical problem, the tool name, browser, a short description and approximate time are usually more useful than the full source file. If a support conversation later requires an example file, the operator should explain why it is needed and how it will be handled before you decide to share it.

SECTION 04 / 10

Purposes and possible legal grounds

Running the requested service

Tool input is used to perform the task you select, such as resizing a picture or calculating a repayment. Website requests are used to deliver pages, assets and downloads and to keep the service available. No additional cloud storage or advertising purpose should be inferred from a tool feature. If a feature changes how data is processed, its description and this policy should be updated before that feature is introduced.

Security and reliability

Where available, access and security records may help identify failed requests, diagnose service errors, investigate abuse and protect the website. That use should be limited to what is reasonably necessary for the issue. The current application does not build behavioural advertising profiles, score people for eligibility or make employment, lending, insurance or similar decisions about visitors.

Optional preference storage

Preference storage and analytics are separate choices. You can allow remembered favourites and theme without allowing analytics, or use every public tool without either. The choice record is stored to respect your decision. If optional Google Analytics is configured and you opt in, it can measure visits, pages, devices, session and country information for audience reports. This is not consent to an email newsletter or advertising personalisation.

Where a lawful basis is required

Where applicable privacy law requires a lawful basis, the operator must identify the basis for each relevant processing activity. Possible grounds can include providing a service you request, a properly assessed legitimate interest in security or support, compliance with a legal obligation, and consent for optional storage where required. These grounds are not interchangeable, and a visitor merely opening a page is not blanket consent to unrelated processing.

Limits and objections

No statement here authorises undisclosed collection or makes a lawful-basis assessment on behalf of an unidentified operator. If processing relies on consent, withdrawal should affect future processing without undoing what was lawful before withdrawal. If processing relies on a legitimate interest and applicable law gives you a right to object, you may raise that objection through the published privacy contact. Some security or legally required records may remain subject to a valid exception.

SECTION 05 / 10

Cookies, local storage and your controls

Storage in the current application

The application uses local storage for your consent choices and, if you allow it, saved favourites and appearance. Optional Google Analytics can set first-party analytics cookies after you enable analytics. The owner-only admin area uses a necessary authentication cookie. No advertising tags are added by this release. Hosting or security services may use their own mechanisms, which the operator must verify; local storage is not automatically sent with every HTTP request.

Specific keys and duration

fixhub-consent records the policy version, preference and analytics choices, and the saved time, valid for up to 180 days. Optional fixhub-favs and fixhub-theme remain until you withdraw permission or clear site data. The necessary fixhub_admin cookie expires after two hours and is used only for admin authentication. When enabled, Google Analytics may set _ga and _ga_* identifiers; this implementation requests a 180-day expiration renewed on consented use. Google account/property retention is managed separately.

Using the controls

On a visit without a valid current choice, allow saved preferences, continue without saving, or open Settings. The settings dialog has separate switches for preference storage and optional analytics, both initially off. The footer reopens it. Withdrawing analytics consent disables further tag collection on the page and attempts to remove this site's analytics cookies. It does not retroactively delete records already sent to Google. You can still use the tools after declining both choices.

Browser and device choices

You can also clear this website's site data through your browser, use private browsing, or block storage. Doing so may remove remembered favourites and theme or cause the choice prompt to appear again. A browser can keep its own cache, history, autofill information and downloads independently of these keys. Use device controls to manage those items. Clearing website preferences does not delete files you downloaded to another folder.

Future tracking

This release can use optional Google Analytics for audience measurement but does not include advertising tags, remarketing or Google signals. The operator can enable collection only by configuring a measurement ID, and visitor analytics permission is still required. Additional marketing or embedded tracking would require a fresh assessment and updated notice. Global Privacy Control does not trigger an advertising-sale workflow here because the application does not sell data or share it for cross-context behavioural advertising.

SECTION 06 / 10

Providers, disclosure and overseas processing

Hosting and delivery

The current website is configured for Node.js hosting on Namecheap. Website requests can be processed by the hosting provider and relevant network, DNS, certificate or security services. The hosting account's actual server region, logs, access controls and backup settings must be confirmed by the operator. The site does not claim that every part of its infrastructure is located in Pakistan or in a visitor's country.

Bundled code and external services

PDF, QR, barcode and ZIP engines are bundled. OCR and background removal download optional code/models from the hosts named on each tool; images stay local. After its separate notice and Start, the Internet Speed Test sends traffic directly to speed.cloudflare.com. Cloudflare receives IP and connection/request metadata and may process network, approximate location and measurement information under its policies at speed.cloudflare.com. Quick/Standard modes plan 13.5/34 MB of payload, excluding overhead. Uploads contain random bytes, not personal files. FixHubLab does not save visitor test results. Optional Google Analytics starts after consent; admin Google reports use restricted APIs.

Email and support providers

Email inquiries are processed by the mailbox providers involved in delivery. Form inquiries are stored on the website host; the form does not automatically send notification email. Authorised admins can view the inbox and manually open a reply in their email application. Google receives any analytics data collected after consent, and its provider terms and privacy information apply to its services. The operator still needs to confirm its mailbox arrangements and any required regional safeguards.

Required or exceptional disclosure

Personal information held by the operator may need to be disclosed when a valid legal requirement applies or when disclosure is necessary and permitted to protect rights, investigate a security incident or respond to abuse. Those possibilities do not create a general permission to sell personal information. The current application has no personal-data sale mechanism, targeted-advertising data feed or data-broker integration.

International safeguards

Hosting, email and optional Google services can involve processing in other countries. Where applicable law restricts international transfers, the operator must assess the destination, recipient and required safeguard. This draft does not assert that a particular agreement or certification has been completed. Consult namecheap.com/legal/general/privacy-policy/ for hosting information and policies.google.com/privacy for Google information. These provider policies supplement this site's explanation rather than replacing it.

SECTION 07 / 10

Retention, deletion and security

Local workspace lifetime

The application holds tool input in the current page or tab so it can process your request. Leaving, refreshing or closing a tool normally removes that page's active workspace. Browser memory, crash recovery, operating-system swapping and extensions can behave differently, so the service cannot promise forensic erasure from your device. Downloaded outputs and print-spool files remain under your control until you remove them.

Preference retention

The consent record is treated as valid for up to 180 days or until the policy version changes. Withdrawing preference permission removes the optional favourite and theme keys. Withdrawing analytics permission stops future analytics collection through this implementation and attempts to remove its cookies. Existing analytics records are governed by the Google property's retention/deletion settings and applicable requirements. Clearing website storage does not remove downloaded files or server-held inquiries.

Operator and hosting records

The application does not configure a precise retention period for provider logs or provider backups. Their actual schedule must be confirmed with the hosting configuration and provider before this draft is finalised. The operator should not retain records indefinitely merely because a limit has not yet been entered. Relevant criteria include the purpose of the record, security needs, legal duties, unresolved disputes, backup rotation and whether the information is still necessary.

Enquiry handling

Contact form messages and their internal notes are retained for 180 days by default. The operator may set a shorter or longer period between 1 and 730 days in admin settings; messages older than that configured period are removed at application start or hourly cleanup. Admins may delete a message sooner. Admin activity records are retained for up to 180 days; admin sessions expire after two hours. Host backups, email messages and exported content backups have separate schedules requiring operator confirmation.

Practical security

The admin area uses hashed passwords, HttpOnly session cookies, request-origin checks and anti-CSRF tokens. Google reporting tokens are encrypted in private application storage; the encryption key must be kept private and backed up securely. A one-time setup key is removed after creating the first admin. These measures reduce risk but do not guarantee security. Use HTTPS, protect hosting access, restrict backup access and avoid sensitive details in blog posts or uploaded public blog images.

SECTION 08 / 10

Your rights, requests and complaints

Rights depend on applicable law

Depending on your location, the operator's activities and the law that applies, you may have rights to learn about processing, access relevant personal information, correct inaccuracies, request deletion, restrict certain uses, receive certain information in a portable form, object to processing, or withdraw consent. These rights are not absolute and do not all apply to every record. The operator should explain any valid exception relied on.

What the operator can access

The operator can access submitted form inquiries and internal notes, published or draft articles, uploaded blog images, website settings, relevant logs and connected Google reports. It cannot retrieve a locally processed tool document from an upload-history database because no such database is provided. A privacy request may concern inquiry information or collected analytics where identifiable and accessible; files and downloads remaining on your device are managed through your device controls.

How to make a request

Use the contact method published on the Contact us page and identify the kind of request. Include only enough information to help locate relevant records, such as the email address used for a previous enquiry and an approximate date. Do not send passwords, full identity documents or confidential files unless a necessary, proportionate verification step has been explained. An authorised representative may need to show their authority where applicable.

Handling and escalation

The operator should respond within the deadline required by the law that applies, verify identity proportionately, and explain any lawful extension or refusal. This draft does not replace different statutory time limits with one universal promise. If an issue cannot be resolved, you may have the right to complain to your competent privacy authority. UK visitors can consult the Information Commissioner's Office; visitors elsewhere can consult their local authority where one has jurisdiction.

An explicit right to object

Where the applicable law gives you a right to object to processing based on legitimate interests, you can raise that objection through the privacy contact. Explain the processing you object to and any relevant circumstances. Continuing to use a tool does not waive an applicable privacy right. Exercising a valid right should not result in unfair treatment or prevent you from using features that do not need the disputed information.

SECTION 09 / 10

Regional information, children and special situations

United Kingdom and European Economic Area

UK and EEA privacy rules do not apply to every website in exactly the same way simply because it is reachable worldwide. Applicability can depend on establishment, offering services to people in those regions, monitoring and other relevant facts. If the operator's activities bring it within those rules, it must assess the appropriate transparency, lawful-basis, transfer, rights and representative obligations. This draft does not claim that an EU or UK representative or a data protection officer has been appointed.

California and other US states

California privacy law provides specified consumer rights for covered businesses, including rights concerning access, deletion, correction and opting out of sale or sharing. Coverage and exceptions must be assessed against the operator's actual circumstances. The current application does not sell personal information or share it for cross-context behavioural advertising. This policy does not claim that a business threshold has been met, create fictional advertising partners or state that every US state uses identical rules.

Canada, Pakistan and other locations

Privacy duties may also arise under laws relevant to the operator, hosting, visitor or activity in Canada, Pakistan or another jurisdiction. The operator must assess those requirements using its verified business details and actual processing. Nothing here promises that a visitor loses mandatory rights because the website is free, hosted overseas or operated under a particular brand. This draft avoids selecting a court or governing law without confirmed operator information.

Children and sensitive information

The tools are general-purpose utilities and are not designed to collect children's profiles or run child-targeted advertising. No age or birth-date field is required by the application. Children should involve a parent or guardian before sharing personal information or sending a message to an unfamiliar service. If you believe the operator has received a child's information inappropriately, use the privacy contact so the circumstances and any applicable deletion duty can be considered.

Shared devices and automated processing

On shared devices, other people may see history, saved preferences and downloaded files. Admins should sign out when finished. Tool calculations do not make eligibility or legal decisions about visitors. Optional analytics produces audience reports rather than a service eligibility decision. The admin Google connection uses read-only reporting scopes; the encrypted access and refresh credentials are for the operator's reporting account and are not public visitor records.

SECTION 10 / 10

Updates, contact and practical reference

Policy changes

The operator should update this notice when purposes, providers or data flows change. This admin release adds stored form inquiries and optional consent-based Google Analytics, so the storage-choice version has been changed and visitors are asked again before optional storage or analytics starts. Published blog content and uploaded cover images are public. New notices should not be used to retroactively justify an undisclosed use of previously collected information.

Contact and request preparation

Contact Fix Hub Lab at info@fixhublab.com for support, privacy requests or press enquiries. The contact details are also published at fixhublab.com/contact. For a privacy request, provide the request category and a concise description. For a tool problem, provide the tool URL, browser and an example using fictional or redacted information wherever possible. Do not include passwords, banking credentials or complete sensitive documents.

Quick actions you can take

To stop optional preference storage, open Cookie settings and choose Continue without saving or switch the preference off and save your choice. To remove downloaded files, use your device's Downloads folder or file manager. To remove browser history, cache, autofill or printer output, use the appropriate browser or operating-system control. To keep an invoice or converted file, save it before closing the tool because there is no cloud account recovery feature.

Current feature checklist

The collection contains 39 browser tools. Images, receipt rows, PDF pages, names, addresses, QR data, barcode values, file contents, CSV data and calculator inputs are processed locally. QR codes embed the information you enter, including any Wi-Fi credentials; share them appropriately. Print generators create documents from your inputs, not official postage, product registration or accreditation. Optional OCR/model downloads are described above; QR, barcode, ZIP and PDF engines are bundled locally. There is no bank connection, checkout or customer cloud-file storage. Owner administration covers blogs, inquiries, SEO and read-only Google reports, with optional GA4 after consent. Download results before closing the page. The collection also includes local reasoning practice and an optional external Cloudflare speed test; see Section 6 for test traffic and provider processing. Product Photo Studio processes its selected photos locally.

Reference and operator review

Primary references include ICO privacy/storage guidance, California Attorney General information at oag.ca.gov/privacy/ccpa, Google's privacy information at policies.google.com/privacy and the hosting provider's privacy policy. These references do not certify this website. Fix Hub Lab uses info@fixhublab.com as its published contact. Hosting region, host log and backup retention, mailbox provider and any required regional arrangements still need confirmation. Check Google property retention separately if analytics is enabled.