DinkSolutions:Privacy policy

From DinkSolutions

This details the data retention policy of this site and how it affects you.

Contents

General Scope

This policy covers personally identifiable information collected or stored by DinkSolutions on its servers in relation to the Projects and their communities. Consistent with its Data Retention Policy, the Foundation collects and retains the least amount of personally identifiable information needed to fulfill the Projects' operational needs.

The public and collaborative nature of the projects

All Projects of the DinkSolutions are collaboratively developed by its users using the MediaWiki software. Anyone with Internet access (and not otherwise restricted from doing so) may edit the publicly editable pages of these sites with or without logging in as a registered user. By doing this, editors create a published document, and a public record of every word added, subtracted, or changed. This is a public act, and editors are identified publicly as the author of such changes. All contributions made to a Project, and all publicly available information about those contributions, are irrevocably licensed and may be freely copied, quoted, reused and adapted by third parties with few restrictions.

Activities on Foundation projects

In general, this Policy only applies to private information stored or held by the Foundation which is not publicly available.

Interactions with the Projects not covered by this Policy include, but are not limited to, aspects of browsing and editing pages, use of the wiki "email user" function, subscribing and posting to Foundation hosted email lists, and corresponding with volunteers via the Foundation's ticketing system ("OTRS"). These interactions may reveal a contributor's IP address, and possibly other personal information, indiscriminately to the general public, or to specific groups of volunteers acting independently of the Foundation.

Users may also interact with one another outside of Foundation sites, via email, IRC or other chat, or independent websites, and should assess the risks involved, and their personal need for privacy, before using these methods of communication.

User accounts and authorship

The Foundation does not require editors to register with a project. Anyone can edit without logging in with a username, in

which case they will be identified by network IP address. Users that do register are identified by their chosen username. Users select a password, which is confidential and used to verify the integrity of their account. Except insofar as it may be required by law, no person should disclose, or knowingly expose, either user passwords and/or cookies generated to identify a user. Once created, user accounts will not be removed. It may be possible for a username to be changed, depending on the policies of individual projects. The Foundation does not guarantee that a username will be changed on request.

Purpose of the collection of private information

The Foundation limits the collection of personally identifiable user data to purposes which serve the well-being of its projects, including but not limited to the following:

> To enhance the public accountability of the projects. The Foundation recognizes that any system that is open enough to allow the greatest possible participation of the general public will also be vulnerable to certain kinds of abuse and counterproductive behavior. The Foundation and the project communities have established a number of mechanisms to prevent or remedy abusive activities. For example, when investigating abuse on a project, including the suspected use of malicious "sockpuppets" (duplicate accounts), vandalism, harassment of other users, or disruptive behavior, the IP addresses of users (derived either from those logs or from records in the database) may be used to identify the source(s) of the abusive behavior. This information may be shared by users with administrative authority who are charged by their communities with protecting the projects.
> To provide site statistics. The Foundation statistically samples raw log data from users' visits. These logs are used to produce the site statistics pages; the raw log data is not made public.
> To solve technical problems. Log data may be examined by developers in the course of solving technical problems and in tracking down badly-behaved web spiders that overwhelm the site.

Details of data retention

General expectations

IP and other technical information

When a visitor requests or reads a page, or sends email to a Wikimedia server, no more information is collected than is typically collected by web sites. The DinkSolutions may keep raw logs of such transactions, but these will not be published or used to track legitimate users.

When a page is edited by a logged-in editor, the server confidentially stores related IP information for a limited period of time. This information is automatically deleted after a set period. For editors who do not log in, the IP address used is publicly and permanently credited as the author of the edit. It may be possible for a third party to identify the author from this IP address in conjunction with other information available. Logging in with a registered username allows for better preservation of privacy.

Cookies

The sites set a temporary session cookie on a visitor's computer whenever a Project page is visited. Readers who do not intend to log in or edit may deny this cookie; it will be deleted at the end of the browser's session. More cookies may be set when one logs in to maintain logged-in status. If one saves a user name or password in one's browser, that information will be saved for up to 30 days, and this information will be resent to the server on every visit to the same Project. Contributors using a public machine who do not wish to show their username to future users of the machine should clear these cookies after use.

Page history

Edits or other contributions to a Project on its articles, user pages and talk pages are generally retained forever. Removing text from a project does not permanently delete it. Normally, in projects, anyone can look at a previous version of an article and see what was there. Even if an article is "deleted", a user entrusted with higher level of access may still see what was removed from public view. Information can be permanently deleted by individuals with access to Wikimedia servers, but aside from the rare circumstance when the Foundation is required to delete editing-history material in response to a court order or equivalent legal process, there is no guarantee any permanent deletion will happen.

User contribution

User contributions are also aggregated and publicly available. User contributions are aggregated according to their registration and login status. Data on user contributions, such as the times at which users edited and the number of edits they have made, are publicly available via user contributions lists, and in aggregated forms published by other users.

No more information on users and other visitors reading pages is collected than is typically collected in server logs by web sites. Aside from the above raw log data collected for general purposes, page visits do not expose a visitor's identity publicly. Sampled raw log data may include the IP address of any user, but it is not reproduced publicly.

Editing projects

Edits to Project pages are identified with the username or network IP address of the editor, and editing history is aggregated by author in a contribution list. Such information will be available permanently on the projects.
Logged in registered users:
Logged in users do not expose their IP address to the public except in cases of abuse, including vandalism of a wiki page by the user or by another user with the same IP address. A user's IP address is stored on the wiki servers for a period of time, during which it can be seen by server administrators and by users who have been granted CheckUser access.
IP address information, and its connection to any usernames that share it, may be released under certain circumstances (see below).
Editors using a company mail server from home or telecommuting over a DSL or cable Internet connection, are likely to be easy to identify by their IP address; in which case it may be easy to cross-identify all contributions to various Projects made by that IP. Using a username is a better way of preserving privacy in this situation.
Unlogged-in registered users and unregistered users:
Editors who have not logged in may be identified by network IP address. Depending on one's connection, this IP address may be traceable to a large Internet service provider or more specifically to a school, place of business or home. It may be possible to use this information in combination with other information, including editing style and preferences, to identify an author completely.

Discussions

On wiki discussion pages:
Any editable page can theoretically be the location of a discussion. In general, discussions on Foundation projects occur on user talk pages (associated with particular users), on article talk pages (associated with particular articles) or in pages specially designated to function as forums (e.g., the Village Pump). Privacy expectations apply to discussion pages in the same way as they do elsewhere.
Via email:
Users are not required to list an email address when registering. Users who provide a valid email address can enable other logged-in users to send email to them through the wiki. When receiving an email from other users through this system, one's email address is not revealed to them. When choosing to send an email to other users, one's email is displayed as the sender.
The email address put into one's user preferences may be used by the Foundation for communication. Users whose accounts do not have a valid email address will not be able to reset their password if it is lost. In such a situation, however, users may be able to contact one of the Wikimedia server administrators to enter a new e-mail address. A user can remove the account's email address from his preferences at any time to prevent it from being used. Private correspondence between users may be saved at those users' discretion and is not subject to DinkSolutions policy.
On mailing lists:
The email addresses used to subscribe and post to Project mailing lists are exposed to other subscribers. The list archives of most such mailing lists are public, and searches of public archives may be performed on the Web. Subscribers' addresses may also be quoted in other users' messages. These email addresses and any messages sent to a mailing list may be archived and may remain available to the public permanently.
Via OTRS:
Some e-mail addresses (such as info-en at wikimedia dot org) forward mail to a team of volunteers trusted by the Foundation to use a ticket system, such as OTRS, to respond. Mail sent to this system is not publicly visible, but volunteers selected by the Foundation will have access to it. The ticket system team may discuss the contents of received mail with other contributors in order to respond effectively. Mail to private addresses of members of Board of Trustees and to staff of the Foundation may also be forwarded to the OTRS team. These messages and e-mail addresses may be saved by members of the OTRS team and any email service they use, and may remain available to them.
On IRC:
IRC channels are not officially part of the DinkSolutions and are not operated on Wikimedia controlled servers. The IP address of users who chat over such a service may be exposed to other participants. IRC users' privacy on each channel can only be protected according to the policies of the respective service and channel. Different channels have different policies on whether logs may be published.

Access to and release of personally identifiable information

Access:

Projects are primarily run by volunteer contributors. Some dedicated users are chosen by the community to be given privileged access. For example, for an English Wikipedia user, user access levels to Wikipedia are determined by the user's presence in various 'user groups'. User group rights and group members are reachable in every project from the Special:ListGroupRights page.

Other users who may have access to private identifiable information include, but are not limited to, users who have access to OTRS, or to the CheckUser and Oversight functions, users elected by project communities to serve as stewards or Arbitrators, DinkSolutions employees, trustees, appointees, and contractors and agents employed by the Foundation, and developers and others with high levels of server access.

Access to and publication of this information is governed by the Access to nonpublic data policy, as well as specific policies covering some of the functions in question. Sharing information with other privileged users is not considered "distribution."

Release: Policy on Release of Data

It is the policy of Wikimedia that personally identifiable data collected in the server logs, or through records in the database via the CheckUser feature, or through other non-publicly-available methods, may be released by Wikimedia volunteers or staff, in any of the following situations:

1. In response to a valid subpoena or other compulsory request from law enforcement,
2. With permission of the affected user,
3. When necessary for investigation of abuse complaints,
4. Where the information pertains to page views generated by a spider or bot and its dissemination is necessary to illustrate or resolve technical issues,
5. Where the user has been vandalizing articles or persistently behaving in a disruptive way, data may be released to a service provider, carrier, or other third-party entity to assist in the targeting of IP blocks, or to assist in the formulation of a complaint to relevant Internet Service Providers,
6. Where it is reasonably necessary to protect the rights, property or safety of the DinkSolutions, its users or the public.

Except as described above, Wikimedia policy does not permit distribution of personally identifiable information under any circumstances.

Third-party access and notifying registered users when receiving legal process:

As a general principle, the access to, and retention of, personally identifiable data in all projects should be minimal and should be used only internally to serve the well-being of the projects. Occasionally, however, the Foundation may receive a subpoena or other compulsory request from a law-enforcement agency or a court or equivalent government body that requests the disclosure of information about a registered user, and may be compelled by law to comply with the request. In the event of such a legally compulsory request, the Foundation will attempt to notify the affected user within three business days after the arrival of such subpoena by sending a notice by email to the email address (if any) that the affected user has listed in his or her user preferences.

The Foundation cannot advise a user receiving such a notification regarding the law or an appropriate response to a subpoena. The Foundation does note, however, that such users may have the legal right to resist or limit that information in court by filing a motion to quash the subpoena. Users who wish to oppose a subpoena or other compulsory request should seek legal advice concerning applicable rights and procedures that may be available.

If the Foundation receives a court-filed motion to quash or otherwise limit the subpoena as a result of action by a user or their lawyer, the Foundation will not disclose the requested information until Wikimedia receives an order from the court to do so.

Registered users are not required to provide an email address. However, when an affected registered user does not provide an email address, the Foundation will not be able to notify the affected user in private email messages when it receives requests from law enforcement to disclose personally identifiable information about the user.

Disclaimer

The DinkSolutions believes that maintaining and preserving the privacy of user data is an important value. This Privacy Policy, together with other policies, resolutions, and actions by the Foundation, represents a committed effort to safeguard the security of the limited user information that is collected and retained on our servers. Nevertheless, the Foundation cannot guarantee that user information will remain private. We acknowledge that, in spite of our committed effort to protect private user information, determined individuals may still develop data-mining and other methods to uncover such information and disclose it. For this reason, the Foundation can make no guarantee against unauthorized access to information provided in the course of participating in Foundation Projects or related communities.

Retrieved from 'http://dinksols.duckdns.org/solutions/index.php?title=DinkSolutions:Privacy_policy&oldid=694'