University of California
CDL
California Digital Library

California Digital Library Privacy Policy

(adopted 2/28/2011)

It is the policy of California Digital Library (CDL) that the privacy of all users will be respected and protected in compliance with federal and state laws and University of California Policies (http://www.ucop.edu/ucophome/policies/bfb/bfbrmp.html). To the extent possible the CDL also conforms to relevant professional standards, as enumerated, for example, by the American Library Association (http://www.ala.org/ala/aboutala/offices/oif/statementspols/statementspolicies.cfm#privacy).

The CDL occasionally collects information from and about users and their interactions with CDL services. The CDL's policy for personally identifiable information (PII)[1] is to: a) minimize its collection; b) to discard or anonymize it as soon as is practical; c) to secure and protect any personally identifiable information that is collected or retained; d) to prohibit its use for commercial purposes; and e) to advocate for, but not guarantee, similar protection by vendors and partners to whose services and content we may direct users.

The CDL discloses personally identifiable information when required by search warrant or subpoena or if there is a substantiated reason to believe that violations of law or of University policies have taken place[2]; or when failure to act might result in significant bodily harm or significant property loss.

All personally identifiable information connected to an individual's use of CDL services is considered confidential. This information includes, but is not limited to, address and other registration information, informational questions asked, and searches, displays, and downloads of content managed by the CDL. This information, however, may be consulted and used by CDL staff in the course of carrying out CDL business.

The CDL examines and may disclose various forms of non-personally identifiable information (e.g. aggregated usage statistics) when there is a business reason or agreement to do so.

This policy applies to all services offered by the CDL. It may be reviewed and revised from time to time (in which case former versions will be made available). Questions about the policy and the practices that support it may be directed to cdl@www.cdlib.org.

Baseline Supporting Practices

(adopted 2/28/2011)

The following practices in support of the CDL's privacy policy apply to all services directly managed and operated by the CDL, except when noted in the privacy policy for that service (typically available from the service's home page).

1. **Limiting Access**. Access to personally identifiable information is restricted to CDL staff who need it to conduct CDL business[3]. University policy (Business and Finance Bulletin RMP-

8 http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html) prohibits University employees and others from "seeking out, using, or disclosing" personally identifiable information without authorization, and requires employees to take necessary precautions to protect the confidentiality of personally identifiable information encountered in the performance of their duties or otherwise.

2. **Permitted access**. When personally identifiable information must be inspected, monitored, or disclosed by court order, subpoena, or University policy, the following shall apply:
   - Authorization. Except in emergency circumstances, such actions must be authorized in advance and in writing by the CDL Executive Director, or by a Director designated by the Executive Director. Authorization shall be limited to the least perusal of content and the least action necessary to resolve the situation.
   - Emergency Circumstances. In emergency circumstances - circumstances in which failure to act might precipitate harm, loss, or liability - any member of the Director's Cabinet may approve the least perusal of content and the least action necessary to resolve the emergency, immediately and without prior written authorization, but appropriate authorization must then be sought without delay.
   - Compliance with Law. Actions taken shall be in full compliance with the law and other applicable University and campus policies. In particular, actions taken in regard to electronic communications, including e-mail, shall comply with the provisions of the University of California Electronic Communications Policy (http://www.ucop.edu/ucophome/policies/ec/).

3. **Informing users**. Except as required by law, users of CDL systems and services are informed whenever personally identifiable information other than transactional information will be collected and stored automatically by the system or service.

4. **Retention**. The CDL retains personally identifiable information only so long as it is required for operational purposes. Where possible PII is discarded or anonymized within 60 days of collection.

5. **Securing systems**. The CDL implements and follows industry standard electronic security measures to secure the systems through which information is collected or stored. Security protections, and all other elements of the CDL's policy, extend to data copies and backups implemented for business continuity.

6. **Other information**. In the course of providing users with web-based services, the CDL routinely collects and stores certain information which is generally not considered "personally identifiable." We use this information on an aggregate basis to maintain, enhance or add functionality to our web-based services. It includes:
   - the user's Internet location, aka IP address (which, depending upon network configuration and practices, may or may not indicate a specific machine regularly used; as a precaution the CDL anonymizes the machine-specific portion of the address per items #4 and #8 of this policy)
   - which pages on our site the user visits
   - the URL of the web page from which the user came to our site
   - which software is used to visit our site and its configuration

7. **Google Analytics and other analysis tools**. The CDL primarily uses Google Analytics to capture and analyze web statistics. Google Analytics is a cookie-based[4] analytics program that uses cookies to track website activity. Google Analytics typically collects, at least temporarily, the following information: Network Location; Hostname; web pages requested; referring web page; browser used; screen resolution; date and time. No personal information is stored within cookies. Cookies can be disabled within a browser's preference or option menu. The CDL's use of Google Analytics includes a standing request that Google anonymize the machine-specific portion of the user's address and that Google cannot share usage data with anyone other than the CDL. In cases where the CDL uses other locally-operated or outsourced web analysis tools, the CDL follows equivalent practice. For more information about Google Analytics, see the Google Privacy Center - Privacy Policy (http://www.google.com/privacy/privacy-policy.html).

8. **Privacy practice audits**. No less frequently than every two years the CDL examines and records the types of PII and usage information that it collects, and confirms its compliance with its privacy policy and supporting practices. Results of these audits are available upon request.

Privacy Protection Limits

1. **End-user responsibility**. Protecting privacy is a shared responsibility. When CDL services require user identifiers and passwords, it is the user's responsibility to use them responsibly, within the policies under which they were issued, and to protect them from misuse by others. Users should not share passwords with any third parties. If a user's password has been compromised for any reason, it should be changed immediately.
2. **Referrals to external sites.** CDL's web services may link to Internet sites and services outside the administrative domain of the library. The CDL does not govern the privacy practices of these external sites. Users should read the privacy statements at these sites to determine their practices. When the CDL contracts with vendors for access to online content, every attempt is made to include user information protections in the license agreement.
3. **Public Records**. Records pertaining to the business of the CDL, whether or not created or recorded on CDL equipment, are University records subject to disclosure under the California Public Records Act, other laws, or as a result of litigation.
4. **Possession of University Records**. CDL employees are expected to comply with requests, properly vetted through University policies and procedures, for copies of records in their possession that pertain to the business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on University electronic communications resources.
5. **Unavoidable Inspection**. During the performance of their duties, personnel who operate and support the CDL's IT infrastructure periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of CDL systems and services. On these and other occasions, systems personnel might observe personally identifiable information. Except as provided elsewhere in this Policy or by law, they are not permitted to seek out such information where not germane to the foregoing purposes, or disclose or otherwise use what they have observed.

   Such unavoidable inspection of personally identifiable information is limited to the least invasive degree of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal and confidential information.

   Except as provided above, systems personnel shall not intentionally search electronic records University's Whistleblower Policy (http://www.ucop.edu/ucophome/coordrev/policy/PP040208Policy.pdf) they shall report violations discovered inadvertently in the course of their duties.

** We acknowledge and thank the UC Berkeley Library and other UC-based privacy statements from which we borrowed inspiration and wording.

[1] Personally identifiable information (PII) is any information that can be directly or indirectly associated with a known individual. Other types of information that the CDL does collect are enumerated in the "Supporting Practices" section of the CDL's privacy policy.

[2] A substantiated reason to believe requires reliable evidence, as distinguished from suspicion, rumor, gossip, or other unreliable evidence.

[3] "CDL business" refers to activities involved in the provision, maintenance, and management of CDL systems and services provided to its patrons and staff. Troubleshooting user interfaces, making usage-based design decisions, and diagnosing problems with underlying technology infrastructure are all examples of CDL business.

[4] A "cookie" is information stored on a workstation by a web server and used to customize a user's interaction with the web. Some cookies last only for the duration of the session, while others are persistent and reside on a computer's hard drive until the user deletes them or the computer is refreshed.