Open Context Privacy Policy

April 21, 2010

Note: This privacy policy closely follows American Library Association recommendations

I. Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. In this system the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a system is in possession of personally identifiable information about users and keeps that information private on their behalf.

The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law. Numerous decisions in case law have defined and extended rights to privacy. Open Context's privacy and confidentiality policies are in compliance with applicable federal, state, and local laws.

User rights—as well as our institution's responsibilities—outlined here are based in part on what are known in the United States as the five "Fair Information Practice Principles." These five principles outline the rights of Notice, Choice, Access, Security, and Enforcement.

Our commitment to your privacy and confidentiality has deep roots not only in law but also in the ethics and practices of scholarly dissemination. Open Context follows the American Library Association's Code of Ethics by protecting each user's "right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted."

II. Open Context's Commitment to Our Users Rights of Privacy and Confidentiality

This privacy policy explains your privacy and confidentiality rights, the steps Open Context takes to respect and protect your privacy when you use its resources, and how we deal with personally identifiable information that we may collect from our users.

1. Notice & Openness

We affirm that Open Context users have the right of "notice"—to be informed about the policies governing the amount and retention of personally identifiable information, and about why that information is necessary for the provision of Open Context services.

We post publicly and acknowledge openly the privacy and information-gathering policies of this system. Whenever policies change, notice of those changes is disseminated widely to our users.

In all cases, we avoid creating unnecessary records, we avoid retaining records not needed for the fulfillment of the mission of the service, and we do not engage in practices that might place information on public view.

Information we may gather and retain about current and valid Open Context users include the following:

- User registration information (only applies to users who tag and annotate Open Context data)
- The Open Context server automatically logs IP addresses for those accessing content; however, we discard IP address information after one month
- Information required to publish content in Open Context (i.e. data contributors and authors)

2. Choice & Consent

This policy explains our information practices and the choices you can make about the way Open Context collects and uses your information. We will not collect or retain your private and personally identifiable information without your consent. Further, if you consent to give us your personally identifiable information, we will keep it confidential and will not sell, license or disclose personal information to any third party without your consent, unless we are compelled to do so under the law or to comply with a court order.

If you wish to publish content in Open Context, we must obtain certain information about you in order to document your project. Users of the Open Context web site may choose to create an account in order to tag and annotate Open Context content; however, creation of an account is not required to search, explore and download content from the system.

In the future, we may collect names, affiliations and email addresses of Open Context users; however, such information will never be required to access Open Context, and will not be distributed to third parties. You may request that we remove your e-mail address or any part of your record at any time.

We never use or share the personally identifiable information provided to us online in ways unrelated to the ones described above without also providing you an opportunity to prohibit such unrelated uses, unless we are compelled to do so under the law or to comply with a court order.

3. Data Integrity & Security

Data Integrity: The data we collect and maintain in Open Context must be accurate and secure. We take reasonable steps to assure data integrity, including: using only reputable sources of data; providing our users access to your own personally identifiable data; updating data whenever possible; utilizing middleware authentication systems that authorize use without requiring personally identifiable information; destroying untimely data or converting it to anonymous form.

Data Retention: We protect personally identifiable information from unauthorized disclosure once it is no longer needed to manage Open Context services. Information that should be regularly purged includes personally identifiable information on resource use.

Tracking Users: We do not ask Open Context users to identify themselves or reveal any personal information unless they are publishing new content or tagging/annotating content already in the system. We discourage users from choosing passwords or PINs that could reveal their identity, including social security numbers.

Third Party Security: We ensure that Open Context's contracts, licenses, and offsite computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. Should a third party require access to our users' personally identifiable information, our agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that personally identifiable information may be disclosed, we will warn our users. When connecting to licensed databases outside the system, we release only information that authenticates users as "members of our community." Nevertheless, we advise users of the limits to privacy protection when accessing remote sites

Cookies: Users of networked computers may need to enable cookies in order to access a annotation services to be made available through Open Context. A cookie is a small file sent to the browser by a Web site each time that site is visited. Cookies are stored on the user's computer and can potentially transmit personal information. Cookies are often used to remember information about preferences and pages visited. You can refuse to accept cookies, can disable cookies, and remove cookies from your hard drive. Open Context servers use cookies solely to verify that a person is an authorized user in order to allow annotation and tagging of resources. Cookies sent by our servers will disappear when the user's computer browser is closed. We will not share cookies information with external third parties.

Security Measures: Our security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Our managerial measures include internal organizational procedures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Our technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and storage of data on secure servers or computers that are inaccessible from a modem or network connection.

Staff access to personal data: We permit only authorized Open Context staff with assigned confidential passwords to access personal data stored in the system for the purpose of performing Open Context work. User passwords will be encrypted with seeded hash algorithm so that Open Context staff will have no ability to read user passwords. We will not disclose any personal data we collect from you to any other party except where required by law or to fulfill an individual user's service request. Open Context does not sell or lease users' personal information to companies, universities, or individuals.

4. Enforcement & Redress

Open Context will not share data on individuals with third parties unless required by law. We conduct regular privacy audits in order to ensure that all programs and services are enforcing our privacy policy. Users who have questions, concerns, or complains about Open Context's handing of their privacy and confidentiality rights should file written comments with the Director. We will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures.

We authorize only Open Context's Executive Editor to receive or comply with requests from law enforcement officers; we confer with our legal counsel before determining the proper response. We will not make Open Context records available to any agency of state, federal, or local government unless a subpoena, warrant, court order or other investigatory document is issued by a court of competent jurisdiction that shows good cause and is in proper form. We have trained all staff and volunteers to refer any law enforcement inquiries to Open Context administrators.