The UC Library Technology Advisory Group (LTAG) recommends that all UC libraries implement the following practices to protect private information in their care. Some of these practices are requirements of federal or state law, while others represent policies or policy recommendations of the University of California or the American Library Association. Detailed references to these laws and policies can be found in the draft "Privacy Audit and Guidelines" issued by the SOPAG Privacy Task Force in August, 2001.

I. PRIVATE DATA RESIDING IN LIBRARY APPLICATION SYSTEMS (INTEGRATED LIBRARY SYSTEMS, ELECTRONIC RESERVES, ELECTRONIC REFERENCE, STAFF DIRECTORIES, ETC.)

A. Circulation and borrower records, including patron registration records, circulation transaction logs, overdue and billing records, records of paging from RLFs and local storage, document delivery & interlibrary loan transactions, and records of access to electronic reserves.

Restrict access to records and logs that reveal what was borrowed by a patron, as well as to patron registration records, to library staff who have a legitimate need to see the records.

Do not allow access to records or logs that reveal what was borrowed, or to patron registration records, to non-library personnel without proper written authorization from the patron or by court order.

Delete patron registration records within 5 years of the expiration of borrower privileges or the last transaction is resolved, whichever is later.

Be aware that the amount of fines or fees owed by a patron may be shared with other campus systems and is subject to the California Public Records Act.

Data kept for statistical purposes should not be capable of being linked to an individual.

B. Records to support personalized services, including search histories saved beyond a session, saved searches and sets, SDI profiles, and files/logs of previous electronic reference queries and answers.

Notify users whenever personally identifiable information (such as name, user ID, email address, etc) is requested and will be stored on the system.

Restrict access to personally identifiable records to library staff who have a legitimate need to consult.

Don’t provide personally identifiable records to a third party without the explicit permission of the patron or by court order.

Regularly purge unused records with personally identifiable information.

If reference answers are kept in a "knowledge bank" for re-use, delete information on the asker before saving.

C. OPAC search logs (see also Web server logs below)

Restrict access to search logs to library staff who have a legitimate need to see the records.

If individual identity is logged, have an online notice advising users that such records exist and privacy can’t be guaranteed.

Data kept for statistical purposes should not be capable of being linked to an individual.

D. OPAC displays of patron borrower records, patron-initiated renewals, and the like.

Allow access to a patron's borrowing record only to the patron.

E. Directory servers that allow user queries.

Treat patron directory information with the same restrictions as patron registration records described above.

For students, don't display any personal information that is not defined as "directory information" on your campus under FERPA.

Block queries about any student who has requested suppression of his/her directory information under FERPA.

F. Directory servers that allow trusted application queries only.

Control access to the directory to trusted applications only

Document clearly what information is provided and to whom

II. PRIVATE DATA RESIDING IN LIBRARY SERVER LOGS

Library Web server logs, including proxy servers, if access is authenticated by user ID.

Notify users that the user ID will be stored in Web server logs.

Restrict access to server logs to library staff who have a legitimate need to consult.

Don't provide server logs to a third party without the explicit permission of the patron or by court order.

Routinely purge log files, keeping only aggregate data for statistics tracking.

Mail message files

Keep files secure and limit access to authorized library systems staff only.

Limit inspection of mail messages by systems staff to the minimum needed for proper functioning and security of the system.

Get proper authorization from the user or a Vice Chancellor, as appropriate, before inspecting any mail messages, or allowing anyone else to inspect mail messages. If the message is from a student, always get advice of counsel as well.

Notify the user if any mail messages are inspected. Notify before inspection except in emergencies.

Purge message files regularly.

C. Mail server logs

Keep log files secure and limit access to authorized systems staff only.

Log only transactional message header information. Do not routinely trap and log mail messages, engage such logging only if required to investigate a specific incident of abuse. If such logs are to be kept, follow same practices as defined above for mail message files.

Purge logs regularly.

III. PRIVATE DATA RESIDING ON LIBRARY PUBLIC WORKSTATIONS

A. Browser caches, including history files

Keep logs secure and limit access to authorized library systems staff only.

Limit inspection of logs by systems staff to the minimum needed for proper functioning and security of the system.

Don't provide logs to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.

B. Cookies & certificates

Keep cookie & certificate files secure and limit access to authorized library systems staff only.

Limit inspection of cookies and certificates by systems staff to the minimum needed for proper functioning and security of the system.

Don't provide cookie & certificate files to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.

C. Operating system logs containing personal information like login ID's

Keep logs secure and limit access to authorized library systems staff only.

Limit inspection of logs by systems staff to the minimum needed for proper functioning and security of the system.

Don't provide logs to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.

Purge logs with personal information frequently.

D. Mail message files stored on public workstations

Keep files secure and limit access to authorized library systems staff only.

Limit inspection of mail messages by systems staff to the minimum needed for proper functioning and security of the system.

Get proper authorization from a Vice Chancellor before inspecting any mail messages, or allowing anyone else to inspect mail messages. If the message is from a student, always get advice of counsel as well.

Notify the user if any mail messages are inspected. Notify before inspection except in emergencies.

If messages are stored locally, purge the mail message files frequently.

E. Paper sign-up sheets

Limit review of sign-up sheets to authorized library staff only.

Keep sign up sheets for a limited period of time

IV. PRIVATE DATA RESIDING ON NETWORK SERVICES

A. Router/switch logs

Keep any traffic logs secure and limit access to library systems staff.

Limit inspection of logs by systems staff to the minimum needed for proper functioning and security of the system.

Don’t provide logs to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.