SILS Phase 4 Data Privacy Task Force
Final Report

Draft of October 19, 2021

Approved by SILS Working Group on October 1, 2021

I. Context

The transition by the University of California (UC) Libraries — the ten campuses, Regional Library Facilities (RLFs), and the California Digital Library (CDL) — to a Systemwide Integrated Library System (SILS) environment will offer new opportunities for data analytics to support decision-making in individual libraries and across the UC system. We believe these opportunities for insight should be encouraged in ways that lead to the development of new services, refining and harmonizing existing services and points of integration with other data lakes and applications operated across the system, enhanced understanding of the impact of the UC Libraries on learning and research, a greater understanding of our patrons, continuous enhancement of services, efficient operations, and compliance with relevant laws and broader UC policies.

Concurrently, the privacy of library patrons needs to be considered alongside the development of such analytics, to safeguard against unauthorized access, inappropriate use, and unintended consequences. This is particularly true as SILS now provides the possibility of one campus library's employees accessing patron data of all campus libraries.

The SILS Phase 4 Data Privacy Task Force (TF) was charged by the Systemwide ILS Working Group (SILS-WG) in March 2021 to clarify and define expectations that will underpin uniform policies and procedures and systemwide governance of local campus data for the SILS.

This report considers only patron data, including circulation data, within the SILS. The UC Libraries consider descriptive data around collections holdings to be factual and therefore public, and so out of scope of this report.

The Task Force has identified overarching policies and practices around use and privacy of patron data. It proposes a path forward enabling the UC Libraries to lead systemwide library initiatives, or projects that support and align UC Libraries needs for assessment and analytics, while complying with University obligations and respecting community expectations around the privacy of patron data.

II. Current Landscape of Policies and Practices

The UC Libraries are committed to protecting the privacy and confidentiality of UC patrons using UC Library Search (the SILS patron interface). Patron data is classified as Protection Level 3 under UC BFB IS-3 Electronic Information Security.

Policies local to each campus library

Individual campus libraries have local policies around the privacy of patron data. They may also have agreements with individual students, faculty, and staff that speak to privacy. At present there is no inventory of these local policies or agreements. The array of data points in this area are numerous and would be complex to collect and analyze.

UC systemwide policies

The UC Libraries are subject to these systemwide policies safeguarding the confidentiality, integrity, and access to data:

- UC BFB IS-3 Electronic Information Security establishes a framework to reduce and manage cyber risk, protect information and support the proper functioning of IT resources. It provides a policy basis to protect user confidentiality; to maintain the integrity of all data created, received or collected by UC to meet legal and regulatory requirements; and to ensure timely, efficient and secure access to information technology resources. Under IS-3, each UC Library is accountable for the information security of its library system, and the data they manage in the SILS environment.

- UC BFB IS-11 Identity Access and Management describes the integration of workflow, process, and technology that enable unique identification of members of the University community and assignment of access privileges, and thus access to resources only by authorized individuals.

- UC PACAOS-130 Policies Applying to the Disclosure of Information from Student Records provide reasonable interpretations of the Federal Family Educational Rights and Privacy Act (FERPA) and protect the student's right of privacy as guaranteed by the Constitution of the State of California and the Information Practices Act. “When the law is silent, the campuses shall be guided by two principles: (1) the privacy of an individual is of great weight, and (2) the information in a student’s file should be disclosed to the student on request.”[1]

- UC BFB RMP-1 University Records Management Program and the UC Records Retention Schedule outlines the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of administrative records, in accordance with relevant law and University policy and practice.

- UC BFB RMP-7 Protection of Administrative Records containing Personally Identifiable Information incorporates the UC Statement of Privacy Values and Privacy Principles and

[1] As a matter of University policy, for the purposes of implementing the provisions of FERPA, the University generally views itself as thirteen separate institutions, rather than as a single entity. The thirteen institutions include the nine general campuses, the one health sciences campus, and the three Department of Energy Laboratories operated by the University. Therefore, personally identifiable information contained in student records maintained by one campus may not be disclosed to the other campuses without the written consent of the student, unless the disclosure is consistent with the provisions of the UC PACAOS-130 policies.

establishes policies around the University's collection, maintenance, safeguarding, and disclosure of personally identifiable information (PII) in administrative records.

Statements

UC Libraries commitment to patrons' privacy and confidentiality has deep roots not only in law and policies but also in the ethics and practices of librarianship. In accordance with the American Library Association's Code of Ethics: "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted." This is consistent with the UC Statement of Privacy Values and the UC Statement of Ethical Values and Standards of Ethical Conduct.

Contractual safeguards with Ex Libris

UC's agreement with Ex Libris includes a negotiated UC Appendix DS – Data Security (dated 12/12/19) that defines how Ex Libris, as the systems supplier for SILS, safeguards data shared by the University and appropriate uses of those data.

III. Governance Recommendations

Governance authority

Recommendation 1: The Council of University Librarians shall have overall responsibility for setting policy with respect to SILS data, with delegations of responsibility to the Direction and Oversight Committee and to the SILS Leadership Group.

SILS data are an asset of the University of California and are to be managed in a manner to further the mission of the UC Libraries and the mission of the University. Data governance is a cooperative effort; the success of data governance efforts depends on collaboration between the UC Libraries.

In addition to the responsibility that the Council of University Librarians (CoUL) already have for SILS systems, CoUL shall have overall responsibility for setting policy and for all aspects of SILS data. The SILS Leadership Group (LG), reporting to the Direction and Oversight Committee (DOC), will act as the CoUL surrogate responsible for oversight of all SILS data with principal responsibility for the establishment of standards and guidelines for appropriately using, managing, and securing those data across the system. The LG should review this SILS privacy and data governance structure periodically, at least once every five years.

Governance of SILS privacy policy, compliance with the policy, and any changes to the policy are the purview of the SILS Leadership Group. SILS privacy policies apply to all library staff and patrons of SILS and any third party with access to SILS data. Each employee with access to SILS patron data has responsibility for understanding and compliance with all privacy related and data use policies. Any SILS privacy policies that are developed by any group should be posted on the SILS Project section under UC Libraries's site and linked to by all participating libraries.

Governance operations

Recommendation 2: A SILS Data Privacy and Security Team should be formed immediately, charged initially to continue with the next phase of this Task Force's work, and then to be convened on an as-needed basis to handle new or complex policy issues.

The Task Force recommends that a standing SILS Data Privacy and Security Team be convened by the SILS Leadership Group to address privacy and data issues as they arise, whether in response to changes in law or policy, new uses of data implicating patron privacy, or as requested by the SILS Leadership Group. The Chair of the team may be self selected or appointed by the Leadership Group. The standing team will provide a well-known focal point for where issues may be referred, consistency and expertise in considering such issues, and making recommendations to the Leadership Group. The Leadership Group may wish to consider having the team provide an annual report summarizing the work of the team over the immediate past year, including the types of issues that were considered and identification of any patterns or trends that may point to a need for reviewing governance or operations.

Team members primarily should have campus expertise in how data is stored and used within library systems, information security, or privacy, or otherwise have knowledge or experience relevant to addressing issues at the intersection of data use, privacy, security, policies, and library systems. The role of SILS Privacy and Security Officer (Recommendation 3) should be a permanent member of the team. The team is expected to seek broader campus input or specific expertise as appropriate.

Much additional planning is needed to operationalize Recommendations 2 (SILS Data Privacy and Security Team), 3 (SILS Privacy and Security Officer), and 4 (Operating Principles). The Task Force thus recommends that the team initially be charged with the following specific deliverables due September 30, 2022, with the expectation it will transition at that time to being convened on an as-needed basis. Deliverables should be submitted to the Leadership Group, as appropriate, as they are completed. During this transition period, the Team should provide informal quarterly progress reports, but raise any major unanticipated implementation issues immediately.

1. Recommendations for operationalizing the decision-making process for privacy and security issues, to include:
    - Criteria for when issues should be brought to the SILS Data Privacy and Security Team and the process for doing so;

    - How the Team considers and develops recommendations, consistent with the Operating Principles in Recommendation 4;
    - How recommendations from the Team are forwarded to the Leadership Group; and
    - How decisions once made are implemented and communicated.
2. Reference templates or documents needed to implement the recommendations made in item 1 above (for example, templates for privacy notices disclosing how the Libraries use patron data or for agreements that can be used when data sharing is contemplated between individual libraries).
3. Recommendations on training that members of the SILS governance (Leadership Group, Operations Team, SubTeams, Groups) should receive as part of their onboarding to become familiar with data privacy and security issues.
4. Any recommendations on refining the Operating Principles in Recommendation 3.
5. A formal report due September 30, 2022.

Recommendation 3: CDL should assign the role of SILS Privacy and Security Officer to an existing staff member from the CDL Operations Center.

A SILS Privacy and Security Officer role should be designated by CDL. There is no expectation for this to be a full-time role, but should be paired with an existing position that has broad oversight responsibilities over SILS.

The SILS Privacy and Security Officer will be a member of the Data Privacy and Security Team and will have responsibility for coordinating with and bringing privacy issues that arise in subteams and other SILS groups to the attention of the SILS Privacy and Security Team, coordinating the documentation of MoUs and agreements centrally, and for operationalizing policies and recommendations developed by the Team (for example, coordination and curation of MoUs or agreements).

This position should receive appropriate training on security and data privacy, particularly around identifying use cases representing new or complex privacy issues requiring escalation.

Operating principles

Recommendation 4: The proposed SILS Data Stewardship Principles should be adopted as the initial operating principles with which SILS patron privacy is aligned.

The new reach of capability for analytics across all UC patron data through SILS carries with it significant responsibilities for the stewardship of these data, many of which possess privacy or confidentiality implications for our patrons and organizational partners. In order to guide our understanding and use of these tools, the Task Force has developed a set of proposed Data Stewardship Principles, consistent with the UC Statement of Privacy Values and Privacy Principles and the UC Statement of Ethical Values and Standards of Ethical Conduct.

1. *Respect for individuals.*

    a. Privacy is a working collaboration between the employees of the entire UC system. We understand that data subjects have the right to know when UC Libraries are processing personal data. We will not conduct analyses which will breach the privacy or rights of our patrons, nor negatively and unnecessarily impact the operations of other units in UC.

    b. When designing analyses or assessments of patron or system generated data, we will adopt a *de minimus* approach at all times, utilizing as little data as possible. Wherever feasible, patron data will be anonymized.

    c. When sharing data with third party suppliers[2], we will consider the impact on patron privacy and where possible incorporate patron consent; patron privacy interests; legal, regulatory and UC policy restrictions or prohibitions; and restrictions on access, use, and disclosure by third parties. Any data access or extracts for external or independent research or analysis must be recorded in a common online database.

2. *Accountability.*

    a. We will retain records of access by our employees of usage data for analytical purposes for a minimum of one year from access, and make them available for inspection for internal system review.

    b. We will conduct regular reviews of employees possessing application account access and restrict or revoke it when it is no longer required.

    c. We will maintain an environment of accountability and utilize audits to ensure that only approved access and analysis of generated application data has occurred.

[2] Definitions from IS-3 policy:

Service Provider: A UC internal organization that offers IT services to Units. Service Providers typically assume most of the security responsibility and help Units understand Unit responsibilities with respect to cyber security.

Supplier: An external, third-party entity that provides goods or services to UC. Section III Subsection 15 of IS-3 policy describes what Suppliers must do. UC has specific contract terms that clarify the responsibilities of Suppliers and protect UC.

3. *Transparency.*

    a. We will develop and maintain consistent notice for all patrons of the data that are gathered on them and their activities; our uses of those data and our data retention periods; and the patron's right to request deletion of their personal data.

    b. We will establish, maintain, and publish notice and response procedures for any occasion of data breach.

4. *Data protection.*

    a. Patron data is classified as Protection Level 3 (P3) under UC BFB IS-3 Electronic Information Security.

    b. UC Libraries will apply security measures commensurate with P3 data when processing patron data.

    c. UC Libraries will ensure appropriate contractual obligations for privacy and information security commensurate with P3 data, including UC Appendix DS – Data Security, with system vendors with which we share patron data.

5. *Review.*

    a. We understand that data privacy requires continual improvement and reflection, and we will review and revise these principles on at least a biannual basis.

IV. Immediate Operational Recommendations

Launching the SILS Data Privacy and Security Team

Charge	● In alignment with the SILS principles, the SILS Data Privacy and Security Team establishes criteria for when issues should be brought to the SILS Data Privacy and Security Team and the process for doing so. It considers and develops recommendations, consistent with the Operating Principles in Recommendation 4 of the SILS Phase 4 Data Privacy Task Force Report; establishes pathways for recommendations to be forwarded to SILS Leadership Group for approval and adoption. And once decisions once made establishes a workflow for implementing and communicating them to the SILS Cohort and campuses. The Team also develops a proposal for implementation for a training (series) that members of the SILS governance (Leadership Group, Operations Team,

	SubTeams, Groups) should receive between Jan 2022 and June 2022 to become familiar with data privacy and security issues. It creates reference templates or documents needed to implement the workflows above (for example, templates for privacy notices disclosing how the Libraries use patron data or for agreements that can be used when data sharing is contemplated between individual libraries). In addition, it provides recommendations on refining the Operating Principles in Recommendation 3 of the SILS Phase 4 Data Privacy Task Force Report.
Timeline	● Group is charged and formed as soon as possible and no later than December 1, 2021, with an 8 month membership. ● Formal report due to SILS LG no later than October 31, 2022.
Reporting Line	● Reports to SILS WG through Dec, 31, 2021. Reporting line switches to SILS LG in Jan 2022.
Team Members* _*not represented. Expertise based._	1. Scott Seaborn (UCB, Campus Privacy Officer, Office of Ethics, Risk and Compliance Services) 2. Kent Wada (UCLA, UCLA Chief Privacy Officer & Director, Policy and Privacy, Office of Advanced Research Computing) 3. Salwa Ismail (UCB, AUL Digital Initiatives and IT, Library) 4. Dale Snapp (UCD, Computing Resource Manager, Library) 5. Imtiaz Haq (UCM, Library Systems Administrator, Library) 6. Gem Stone-Logan (CDL, SILS Senior Systems Analyst) 7. Caitlin Nelson (CDL, SILS Services Manager)

Addressing Specific Issues

Alma/Primo Privacy Form	● We request the SILS PMs work with the ICs to ensure that every staff member on every single campus, RLF, and CDL, who has an Alma or Primo account, sign the privacy form (retroactively and moving forward) by Dec 1, 2021. And every single member on any campus, RLF, or CDL who gets an Alma account is made to sign the form by that campus's Alma account giving person to ensure that the privacy form is signed before an account is given at the IZ or NZ level. The response spreadsheet for this privacy form could be shared view-only with the campus's point person who gives out the account, so they can confirm that the staff member has signed the form and give out the account without asking PMs (who own the form) if it has been signed.

Anonymizing User Information Analytics	● Ask CDL NZ administrator to ask ExL to flip the switch to anonymize the “person” to just retain the FN, LN, identifier for now (link1, link2). ● Request that CDL NZ administrator work with ExL to help us understand this issue and make this the first priority for the new SILS DS PT to resolve.