Information on University Use of Work-Related Data

In Resolution 2023-3, "On Endorsing Principles for Work-Related Data," the Faculty Council asked for comment and assurance from the University administration on several points. The Faculty Council notes the growing volume of data "footprints" created simply by doing work. These data include content and metadata. The resolution articulates concern that these data may be collected and used in ways not originally intended, and maybe in ways the individual might not prefer. We share this concern. We endeavor to operate responsibly with respect to it, yet also satisfy the University's legal, ethical, contractual, and other constraints in how it collects, uses, and shares data.

These are fruitful topics and the opportunity to engage is welcome. To initiate that engagement, we sketch initial comments here:

1. **Transparency**:
    a. Explain what data are and are not collected.

Electronic information consists of content and activity data. Each system collects data specific to its function and purpose. For example, Canvas would hold curriculum and course content, and would include data associated with its specific tooling—gradebooks, discussion boards, assessments; Microsoft365 holds email, calendaring appointments, documents/files in OneDrive; ConnectCarolina contains financial transactions, student registration/enrollment, and human resources related data.

With respect to metadata, by policy, systems containing most of the work of the University collect activity data, including: access logs (for example, login/exit as well as logs of activity in the system); and system logs for troubleshooting that often contain activity records. Network traffic is logged in various ways (for example, firewall logs at least, and more sophisticated systems looking for malware and other security issues log enough to look for patterns). This kind of activity data is needed for IT staff to perform essential functions, including security incident response, system protection, maintenance and management activities, to ensure they comply with regulatory and contractual obligations, and to protect against security threats such as cyberattacks, malware, and phishing.

University IT resources also require regular management, for example, to deploy software updates. To perform this work, the University and its approved vendors may scan and otherwise access electronic information without user consent. In carrying out these processes, University IT personnel may observe activity data or other electronic information. Even so, University IT personnel are limited to the minimum amount of unavoidable examination of electronic information necessary to perform such duties. Except as otherwise provided by University policy or law, University IT personnel are not permitted to seek out electronic information, including contents or activity data, when not germane to system operations and support. In addition to protecting the electronic information itself, these limitations protect University IT personnel from being directed to access electronic information beyond those limits, or for purposes other than those permitted or required by University policy or law.

    b. For the data that are collected, explain how they may be used.

Data are collected and used primarily for their original purpose. Content in any University system is, and should be, used to advance the mission of the University.

As described above, University IT resources require ongoing system protection, maintenance and management activities to ensure they are operating properly (for example, deploying software patches), meeting regulatory and contractual obligations, as well as protecting against security threats. Also as described above, any unavoidable examination of electronic information is limited to the minimum required to perform such duties. Hence, though the University and its approved vendors may scan or otherwise access electronic information without user consent in performing these systems operations and support activities, the University and its approved vendors may do so only to the minimum necessary to discharge these essential functions.

In accordance with applicable University policy and law, University IT personnel are not permitted to use or seek out electronic information, including contents or activity data, when not germane to system operations and support activities. Notably, this exception does not exempt information systems personnel from the prohibition against disclosure of personal or confidential information otherwise protected by applicable University policy and law, including: Acceptable Use Policy, Administrative Systems Terms of Use Policy Information Classification Standard, Data Governance Policy and Standard, etc.

These safeguards protect both the electronic information itself and protect IT (and other personnel) from being directed to access electronic information beyond authorized limits, or for purposes other than those permitted or required by University policy or law.

c. Notify faculty when significant changes are made to data practices that could be used to assess performance.

The updated Policy on Access to Individual User Accounts limits access to digital data to specific objectives which do not include routine reviews of job performance.

Systems operated by ITS do not log nor collect metadata for the purpose of assessing performance. Absent a legal requirement to do so, in University systems operated by ITS a request to use those data for the purpose of assessing performance would be a change from the original intent and would therefore be denied and referred for data governance review.

The Office of Human Resources is the appropriate authority if employees or supervisors have questions about what is and is not an appropriate method of performance assessment. They have no current nor foreseeable plan to look at nor recommend the use of interaction data to evaluate performance.

Assessing faculty performance is a complex matter that encompasses variations due to areas of study/expertise, professional practice standards, tenure and promotion policies, adherence to human resources guidelines, applicable state, local, and federal law, etc.. With that said, the Office of the Provost fosters an environment where faculty are fully informed of the criteria of their evaluation, and the materials that will be used as evidence pertaining to those criteria, in advance of that evaluation: at the time of recruitment, periodically during departmental meetings, at the beginning of evaluation periods, and as reminders as assessment outcomes are shared. Hence, if an evaluator wishes to include data as evidence against an assessment criterion he/she/they should discuss that in advance with his/her/their faculty, with academic officers in his/her/their academic unit. Note, too, that the evaluator would be required to request access to these data, which would then be reviewed by appropriate institutional authorities under the applicable policies and rationales.

d. Clarify whether data are stored on university systems or third party systems,

The University's information systems are composed of both on-premise (maintained at the University) and third-party components. Systems are considered University systems whether they are owned and operated by the University or are licensed "cloud" applications doing the work of the University. When the University contracts with outside vendors that will have access to Tier 2/3 personally identifiable electronic information to perform services on behalf of the University, the University requires an information security review must be performed to ensure the vendor meets minimum security standards. Additionally, the University requires appropriate service contracts to be in place that limits the third-party contractor from using University data for any purpose other than to perform the services of the agreement or as required by law. When data are in on-premise systems, IT staff have a rigorous set of requirements to protect the data and provide only authorized access.

e. the expectations for how long most kinds of data are stored,

Data of all kinds are stored for durations that comply with the University Records Retention and Disposition Schedule. In practice that usually means they are stored while they have business value (their original intended use) plus some duration. If they are subject to other requirements, they may be stored for a longer duration driven by the requirement itself. If they are transferred to University Archives according to the Records Schedule, how long they are retained becomes a curation decision.

f. information about who has access to data and in what circumstances.

By policy, every University information system (whether built, managed, or maintained by University staff, or licensed from a third-party) is required to have reasonable and appropriate access measures in place to limit access to University data only to those persons or automated processes that have been granted access rights based on their required functions (role-based access), while preventing those who have not been granted those rights from obtaining access to University data.. *See* ; Access Control Standard. Access controls to University systems correspond to the sensitivity level of the data maintained on the system. *See* Information Security Controls Standard; Information Classification Standard. In accordance with University policy, the information system authority for a particular system will only grant access rights to those persons or automated processes (e.g., interfaces between two information systems) that have a legitimate business need based on the current responsibilities or function to access the information system. *See* Policy on Terms of Use for Administrative Systems, Information Security Control Standard, Minimum Necessary Standard.

It is important to note that the University is subject to public records laws and obligated to produce public records as applicable. *See* Policy on Public Records Requests. These laws apply to records created or received in connection with the transaction of University business, in whatever format, and are not scope restricted only to University-owned devices or University-sponsored services. I.e., sending, receiving, storing, etc., This means that carrying out University business through personal email, personal phones, on personal computers does not change the ownership of any records created or received in connection with University business nor the University's obligation to produce/release them.

g. Confirm and communicate procedures for decision making regarding data collection and sharing.

When large systems are established, the people building them work with stakeholders, which should include representatives of customer communities. Communication among members of the University community is essential for University operations, teaching, research, and public service endeavors.

To that end, the University has established policies, procedures and practices to collect, use and share data, including: Administrative Systems Terms of Use Policy, Access Control Policy, Access Control Standard, Information Security Control Policy, Information Security Control Standard, Data Governance, Minimum Necessary Standard.

Some units of the University are established to be responsible for some kinds of data use and sharing. The Public Records Office, University Archives, and Internal Audit, have permission to receive data to accomplish their mandates. The Office of University Counsel handles other types of data for litigation and other purposes. Each of these offices has established practices for data handling in compliance with applicable law and policy.

h. Establish and communicate a clear chain of decision making regarding use of data.

The individual is the first stop when data in individual accounts is needed. In some circumstances that isn't the right path, and a structure exists to address those situations.

With respect to metadata about work activity, those data follow a similar flow as any other data type. Consider Student data. Staff may share that data for purposes defined in FERPA, routine flow of data. But when unusual uses arise, permission is needed. The same is true for IT data. Technical and other staff responsible for systems may share that data in the course of their regular work. But if requested by someone else, a determination is needed.

When new questions arise about appropriate data sharing and use, those can be vetted through the Data Governance Oversight Group. Metadata in systems is "IT data." The CIO is the Data Trustee for that type of information and sets rules for its use. ITS anticipates publishing a formal Standard to clarify some of these questions and provide consistency between ITS and unit IT responses.

2. **Prohibit Surveillance**:
   a. Ensure that data requests can only be made based upon accepted grounds with a documented rationale (e.g., for public records, public safety, network protection, or authorized legal matters).

Administrators and staff do not conduct active surveillance using UNC digital data. Data are sometimes requested retrospectively following established and longstanding procedures. Though business justification is part of that requirement, a role-based gate is used, and authorized requestors adhere to the Administrative Systems Terms of Use Policy, which has rigorous requirements when accessing University Data. In cases where an authorized role-based gate is used and ITS staff are not privy to the rationale, ITS will document/record the fact that the role-based gate was used, and by whom; in the forthcoming formal Standard, the CIO anticipates including this guidance for IT staff in units outside of

ITS. In such a case, the onus is on the authorized requestor to document/record the rationale for the request. Referral to data governance for review is also available, if warranted.

When the University has warrant or obligation to access contents without notifying an individual—e.g., when the University looks at data as part of an investigation—the assessment is based on a search of key terms and attributes that are salient to the investigation. The assessment is not a wholesale unrestricted review: it is bounded, by keywords and other scope-specifying parameters, to the scope of the investigation.

b. Confirm and communicate policies limiting the use of data for job performance decisions.

Please see remarks above regarding use of data for assessing faculty performance. The updated Policy on Access to Individual User Accounts limits access to digital data to specific objectives which do not include routine reviews of job performance.

c. Confirm that faculty retain intellectual freedom in public digital spaces and that any monitoring of social media is conducted to support public safety, and will not be used to target specific groups or individuals or for political purposes.

Intellectual freedom requires that faculty and other employees have the freedom to express themselves on social media platforms. Should IT staff receive inappropriate requests for this sort of activity, they have avenues to report through their HR representative, EthicsPoint, and other options.

d. When requests for data are made and/or social media monitoring is conducted, individuals involved should be notified when legally permissible.

The University endeavors to notify individuals when it is legally permissible and would not compromise the integrity of a suitably authorized investigation.

3. **Privacy and Data Ownership**:

a. Highlight the rights that faculty have over their own data.

The University approaches data protection from a “University Data” perspective. Whether data is owned by the University, faculty, or someone else, if it is in some form of University IT, or is being received, created, or used for the business of the University, then all data governance, protection, sharing, and use policies apply to it. The University will protect faculty data as rigorously as any other data, and establish access control and permissions, negotiate contracts with third parties to include data protection measures, and otherwise manage the data professionally.

b. Make clear when data are “owned” by the University and when they are the intellectual property of faculty.

Faculty production of scholarly works, pedagogical materials, and other intellectual property is protected by all relevant copyright law, whether or not the works are stored on University servers, However, the guarantee of confidentiality or privacy is limited by applicable University access policies.

Further, the University enters into contractual agreements with agencies and third parties that have a bearing on it. While there are generalities that usually apply, the range of individual and special cases is vast. This is a complex topic with multiple laws, regulations, contractual agreements, and other constraints.

c. Make public any instances of sale or sharing of data by the University.

“Sale” of data and “sharing” data are significantly different. In general, the University shares data only when we are required to do so—for example, to the federal government for financial aid purposes or other compliance purposes, to the UNC System Office for reporting purposes, to accrediting entities, etc.. Such sharing is governed by the issuing authorities via various means, whether law, policy, regulation, and so on. In cases where the University shares data with a third-party for delivery of some service or function—for example, we share with Microsoft our authorized user population for providing access to Microsoft365; or, we share with Adobe the authorized users for Adobe Creative Cloud—the terms and conditions are covered by contract which we negotiate to limit their secondary uses.

With respect to “sale” of data, any such activity would be processed with legal review and with support of appropriate administrative and operational offices including the Office of Technology Commercialization, the Office of Industry Contracts, and the Institutional Privacy Office, to ensure that sale of data is permitted by applicable law and University policy.

d. Educate faculty on individual rights and appropriate processes related to the sale or use by others of their data.

Please see safecomputing.unc.edu for information of this kind.

e. Confirm that data related to instructional materials (e.g., syllabi and assignments) constitute faculty intellectual property.

See comments on intellectual property with respect to “data”, above.

f. Clarify faculty intellectual property rights for various categories of research (sponsored, individual, collaborative).

See comments on intellectual property with respect to “data”, above.

g. Ensure that contracted third-parties have no or appropriately limited access to faculty data and that contracts delineating third party uses of faculty data are available for review upon request.

Other than required public records disclosure, and published information like the University Directory, the University has controls over sharing employee data. The niversity scrutinizes third parties for data security and protection measures and subjects the agreements to legal review when contracting for services involving employee data.

4. **Promote Education**:
   a. Create easy access to documentation and policies for work-related data.

ITS intends to publish a formal Standard addressing many of the concerns identified here, and describing how IT and other staff can comply with the Individual Accounts Policy. All University policies are available on policies.unc.edu. See safecomputing.unc.edu, Carolina Talent, and datagov.unc.edu for training and information on data protection.

If you have specific questions or would like for someone to talk with a group about data-related policies, feel free to email its_policy@unc.edu to set something up.

b. Charge campus entities (e.g., Information Technology Services, The Office of Legal Counsel, University Archives, The Office of Ethics and Policy) with educating campus constituencies about data concerns and rights.

Thank you for asking! In addition to the annual security training, and a host of activities throughout the year from the Information Security Office (have you subscribed to the "Data At Rest podcast?") many ITS staff are available to speak to groups on topics of data concerns of many kinds. In addition, ITS Communications provides articles in its own publications and through The Well and other campus outlets.

ITS Information Security Office also sponsors the Information Security Liaison (ISL) program. Your unit should have one or more ISLs available to answer questions about data and to help you find resources to answer questions they can't.

The Enterprise Data Coordinating Committee is responsible for campus training efforts and for building structure around University Data use. The Data Governance Oversight Group has resources available for guidance on questions about data (link at the bottom of each datagov.unc.edu page).

The Institutional Privacy Office provides training annually to all "workforce" in HIPAA Covered Units that relates to data concerns.

The Digital Accessibility Office has rich training available through Carolina Talent on topics related to data concerns and rights. They also support units in good data practices. Regardless of ownership, the DAO is intensely interested in helping faculty to shape their course materials in ways that make them the most universally usable they can possibly be.

c. Develop programs for providing and updating training related to data for units and faculty.

The Information Security Office, Institutional Privacy Office, Enterprise Data Coordinating Committee, Digital Accessibility Office, and others have established training programs and update their training regularly (or at least occasionally in some cases). Suggestions for topics and assistance spreading the word about training are always welcomed!

Reading List:

Information Classification Standard

Data Governance Policy and Standard

Acceptable Use Policy

Administrative Systems Terms of Use Policy

Copyright Policy

Individual Accounts Policy (new)

Individual IT Data Standard (upcoming)

Datagov.unc.edu

Safecomputing.unc.edu

NC 132 Public Records