UNIVERSITY SENATE | LEGISLATION APPROVAL | #20-21-15

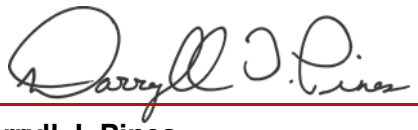
Approved by the Senate on December 9, 2021

Proposal to Establish a University Privacy Policy (Senate Document #20-21-15)

TO **Darryll J. Pines | President**

FROM **Ellen D. Williams | Chair, University Senate**

I am pleased to forward the accompanying legislation for your consideration and approval. Derek Richardson, Chair of the University IT Council, presented the Proposal to Establish a University Privacy Policy (Senate Document #20-21-15), which the University Senate approved at its meeting on December 9, 2021. Please inform the Senate of your decision and any administrative action related to your conclusion.

Approved:  **Date:** 12-22-2021

Darryll J. Pines
President

Copies of this approval and the accompanying legislation will be forwarded to:

Jennifer King Rice, Senior Vice President and Provost
Reka Montfort, Executive Secretary and Director, University Senate
Michael Poterala, Vice President and General Counsel
Dylan Baker, Interim Associate Vice President for Finance and Personnel
John Bertot, Associate Provost for Faculty Affairs
Elizabeth Beise, Associate Provost for Academic Planning & Programs
Rhonda Smith, Acting Director, Academic Affairs
Derek Richardson, Chair, University IT Council
Jeffery Hollingsworth, Vice President and Chief Information Officer
Joseph Gridley, Director and Chief Data Privacy Officer
Mary Shelley, IT Security Advisory Committee Chair

UNIVERSITY SENATE | TRANSMITTAL | #20-21-15

IT Council

Proposal to Establish a University Privacy Policy

PRESENTED BY	**Derek Richardson, IT Council, Chair**
REVIEW DATES	**SEC – November 22, 2021 | SENATE – December 9, 2021**
VOTING METHOD	**In a single vote**
RELEVANT POLICY/DOCUMENT	**N/A**
NECESSARY APPROVALS	**Senate, President**

ISSUE

In fall 2020, a proposal was submitted to the Senate Executive Committee (SEC) related to the creation of a new University Privacy Policy. The proposal noted that the University lacked a formal Privacy Policy, and that the lack of such a policy could lead to the University's inability to meet regulatory compliance obligations, as well as a potential inability by the University to obtain grant funding. In April 2021, the SEC voted to charge the IT Council to review the proposal, related regulations and policies, to benchmark with peer institutions, propose a new policy, and consult with University stakeholders on the proposed policy.

RECOMMENDATION(S)

The IT Council recommends that the proposed University of Maryland Privacy Policy, as shown immediately following this report, be approved.

COMMITTEE WORK

The IT Council began its review of the charge in April 2021. The Council agreed to task the IT Security Advisory Committee (ITSAC) with fulfilling the elements of the SEC's charge. The ITSAC consulted with the proposer (the Chief Data Privacy Officer), the Vice President for Information Technology & Chief Information Officer (VPIT & CIO), the Office of General Council, and stakeholders across administrative, academic, and research units, including Senate staff, to develop a draft privacy policy. The Committee also reviewed peer institution policies and best practices. After a preliminary draft of the policy was developed utilizing feedback from individual employees and students, departments, colleges, and senior leadership, it was made publicly available via a campus-wide notification, and five open forums were held in September 2021. Community feedback from these forums was incorporated into a more detailed draft policy, which was presented to the Senate at its October 2021 meeting to solicit preliminary feedback before the policy could be finalized. Additional feedback from Senators and the Senate Chair was incorporated into a final draft of the policy that the ITSAC submitted to IT Council in November for approval. The IT Council unanimously approved the proposed new privacy policy at its meeting on November 10, 2021.

Throughout drafting and feedback cycles, several subjects were given deep consideration by the ITSAC including the applicability of the policy; defining the University's core Privacy Principles; equity as a privacy principle; expectation of Privacy granted by the policy; relationships between the proposed policy, privacy-related regulations, and existing University policies that directly address such regulations, the forthcoming standards; exceptions to the policy; and whether and how policy violations should be addressed within the proposed policy.

IT COUNCIL REVIEW

Members of the IT Council participated in, or were briefed about, each of these conversations throughout the drafting and feedback process, and were granted real-time opportunities to provide their own input. Further, the November meeting of the IT Council was devoted entirely to exploring and reaffirming the decisions made on each of the issues identified by the committee. The IT Council unanimously voted to approve the proposed new policy at its meeting on November 10, 2021 and subsequently approved two technical revisions to remove placeholder links from the policy on December 1, 2021.

ALTERNATIVES

The Senate could choose not to approve the proposed new policy. However, doing so would continue to put the University at substantial risk with regard to compliance with regulatory and contractual requirements.

RISKS

There are no risks to the University in adopting the proposed policy.

FINANCIAL IMPLICATIONS

Adoption of the proposed policy is likely to create new and/or updated institutional processes that may require leveraging existing resources in new ways or additional resources.

Proposal to Establish a University Privacy Policy

2021-2022 Committee Members

Derek Richardson (Chair)
Yifei Mo (Faculty)
Jim Zahniser (Faculty)
Julie Wright (Exempt Staff)
Philip Piety (Faculty)
Mary Shelley (Exempt Staff)
Jonathan Resop (Faculty)
Peter Keleher (Faculty)
Lisa Peterson (Exempt Staff)
Eunha Yim (Graduate Student)
Hallie Oines (Undergraduate)
Jeffrey Hollingsworth (Ex-Officio)
Axel Persaud (Ex-Officio)
Marcio A. Oliveira (Ex-Officio)
Joseph Gridley (Ex-Officio)
Gerry Sneeringer (Ex-Officio)
Jack Blanchard (Ex-Officio)

Date of Submission

November 2021

BACKGROUND

In fall 2020, a proposal was submitted to the Senate Executive Committee (SEC) related to the creation of a new University Privacy Policy. The proposal noted that the University lacked a formal Privacy Policy, and that the lack of such a policy could lead to the University's inability to meet regulatory compliance obligations, as well as a potential inability by the University to obtain grant funding. In April 2021, the SEC voted to charge the IT Council to review the proposal, related regulations and policies, benchmark with peer institutions, propose a new policy, and consult with University stakeholders on the proposed policy.

COMMITTEE WORK

The IT Council began its review of the charge in April 2021. The Council agreed to task the IT Security Advisory Committee (ITSAC) with fulfilling the elements of the SEC's charge. The ITSAC consulted with the proposer (the Chief Data Privacy Officer), the Vice President for Information Technology & Chief Information Officer (VPIT & CIO), the Office of General Council, and stakeholders across administrative, academic, and research units, including Senate staff, to develop a draft privacy policy. The Committee also reviewed peer institution policies and best practices. After a preliminary draft of the policy was developed utilizing feedback from individual employees and students, departments, colleges, and senior leadership, it was made publicly available via a campus-wide notification, and five open forums were held in September 2021. Community feedback from these forums was incorporated into a more detailed draft policy, which was presented to the Senate at its October 2021 meeting to solicit preliminary feedback before the policy could be finalized. Additional feedback from Senators and the Senate Chair was incorporated into a final draft of the policy that the ITSAC submitted to IT Council in November for approval. The IT Council unanimously approved the proposed new privacy policy at its meeting on November 10, 2021.

Throughout drafting and feedback cycles, several subjects were given deep consideration by the ITSAC. The applicability of the policy arose as a critical question. As the proposed policy is intended to address all collection, processing, and use of the information of any identified individual, the ITSAC took great care to clarify that the policy applies regardless of the relationship of a data subject to the University, regardless of the origin of the data, regardless of the affiliation an

individual may have with the University, and regardless of the purposes for which information may be used.

Defining the University's core Privacy Principles was also a critical conversation. Of key interest were the principles of Transparency and Equity. After much discussion and feedback, the ITSAC chose to describe the principle of Transparency as an individual's ability to discover the purpose for which their data may be used, as well as information regarding the collection, storage, and use of such information. The ITSAC explored whether Transparency was suitably addressed by making information available upon request of an individual, or whether Transparency could only be achieved through proactive notice to an individual each time their data was to be used. It was ultimately decided that proactive notice to each individual each time their data was used was infeasible in practice, and was likely to create an environment in which such notices would become noise to be ignored. The return.umd.edu Data Use Policy was reviewed and held as an exemplar of appropriate Transparency in the absence of individual notifications.

Equity as a privacy principle was carefully considered, specifically in regard to what the principle may address in practice. Equity was discussed in the context of the impact that collection and use of certain data elements, including but not limited to demography, could have on an individual; given that improper use of identifiable information can represent a significant risk of harm to individuals and perpetuate systemic inequalities, it was determined that Equity considerations in the collection and use of information should be addressed as a core principle.

Much discussion was also had by the ITSAC and stakeholders with regard to the Expectation of Privacy granted by the policy. It was recognized that some expectation of privacy was critical to the promotion of academic freedom and furtherance of the University's mission. However, it was also noted that certain regulatory regimes, including the Maryland Public Information Act, restrict that expectation of privacy. Further, it was recognized that the University has obligations to its community to protect the health and safety of its members, the integrity of its academic offerings, and the responsible stewardship of the funds it receives. As such, the policy both grants a reasonable expectation of privacy while also reserving the right for the University to access and use PII to investigate misconduct or other risks to the University community. It was acknowledged and considered important to note that the University's right in this interest remains subject to the privacy principles and operational standards that will balance the University's obligations with the privacy rights of its data subjects.

Discussion was also had regarding the relationships between the proposed policy, privacy-related regulations, and existing University policies that directly address such regulations. Great care was taken to ensure that the framework set forth by the proposed policy and its forthcoming standards will guide the interpretation and implementation of regulatory obligations and existing policies. Among broader discussions, the ITSAC and its stakeholders discussed the interplay between this policy and existing policies that address healthcare information, student data, financial information, and personnel records. It was concluded that the principles and expectations of the proposed policy, as well as its implementing standards, would set the way privacy-related regulatory or policy requirements, such as the evaluation of "minimum necessary use" and "legitimate interest", would be accomplished.

The forthcoming standards were also an issue of critical concern. The ITSAC recognized that the abstract nature of privacy principles and expectations requires operational requirements to provide the University community assurance not only that they were acting in compliance with the policy, but also that the University itself would be held to the principles and expectations. It was determined

that the proposed policy should follow the model of the University's Policy on the Acceptable Use of Information technology Resources, which allows for the issuance of Standards to supplement the policy. It was important to note that such standards have the potential to impact many individuals, units, and activities at the University; as such, it was determined that the policy should specifically address the need for the Vice President for Information Technology & Chief Information Officer to coordinate the development of such standards with the IT Council and other appropriate University stakeholders.

Exceptions were also considered a key component of the proposed policy, as unanticipated events or uses of data may arise that have the potential to conflict with the policy's principles or expectations. The use of wireless log data to establish COVID-19 testing compliance was considered as an exemplar of a use of data that exceeded the anticipated purpose for which the data was collected, yet served a critical enough health and safety purpose to require an exception to the principle of Limitation. Importantly, it was noted that such exceptions will require official requests that must be reviewed by a group of stakeholders, and such requests must evaluate the purpose for the exception in context of any risks to the privacy of the individuals that may be impacted.

Finally, robust discussion was had related to whether and how policy violations should be addressed within the proposed policy. The ITSAC discussed this issue with several stakeholders and received significant feedback. It was noted that individual violations of the proposed policy should remain subject to standard University procedures related to employee or student misconduct. However, further discussion was had regarding the potential University-wide impact of individual or unit-level violations. It was determined that, while the proposed policy should not change any processes or procedures related to individuals' violations, the Policy should establish and clarify the responsibility that a unit is subject to in the event that a Unit Head knowingly or intentionally violates a policy on behalf of their unit where such a violation results in externally imposed costs, whether such costs are a result of regulatory fines or data breach remediation costs. It was, however, carefully noted that such a responsibility should only result from a deliberate decision. Further, it was noted that it may not be feasible or appropriate for a unit to cover the entire cost associated with a breach or fine, which resulted in the insertion of language to clarify that the unit may only be responsible for a portion of such costs.

IT COUNCIL REVIEW

Members of the IT Council participated in, or were briefed about, each of these conversations throughout the drafting and feedback process, and were granted real-time opportunities to provide their own input. Further, the November meeting of the IT Council was devoted entirely to exploring and reaffirming the decisions made on each of the issues identified by the committee. The IT Council unanimously voted to approve the proposed new policy at its meeting on November 10, 2021.

The IT Council voted to approve two technical revisions to remove placeholder language for hyperlinks from the policy on December 1, 2021.

RECOMMENDATION

The IT Council recommends that the proposed University of Maryland Privacy Policy, as shown immediately following this report, be approved.

APPENDICES

Appendix 1 — Charge from the Senate Executive Committee

Appendix 2 — Privacy Policy Peer Institution Comparison

Proposed New Policy from the IT Council

X-15.00(A) UNIVERSITY OF MARYLAND PRIVACY POLICY
Approved by the President [December X, 2021]

I. Introduction

The University of Maryland, College Park ("University") values and embraces the ideals of freedom of inquiry, freedom of thought, and freedom of expression, all of which must be sustained in a community of scholars. The University encourages, supports, and protects freedom of expression, an open environment to pursue scholarly inquiry, and the open exchange of ideas and information. These values lie at the heart of our academic community.

The University must balance free expression with the institutional obligations of each member of the campus community to collect and use Personally Identifiable Information ("PII") responsibly, ethically, transparently, and in a manner that both accords with the law and respects the rights of individuals. The University depends on a shared spirit of mutual respect and cooperation in order to create and maintain a culture of respect, equity, transparency, and responsibility.

Similarly, the University must balance the pursuit of its academic, research, and service missions and its legal, administrative, research, and academic responsibilities with its obligation to collect and use PII responsibly, ethically, transparently, and in a manner that both accords with the law and respects the rights of individuals.

In order to uphold these values, this Policy has been established as a framework for compliance, responsibility, and accountability as it relates to an individual's Privacy Rights, with regard to the collection, use, and protection of PII.

II. Definitions

A. "Personally Identifiable Information" means information that is created, received, processed, stored, or transmitted by or on behalf of the University that, alone or in combination with other information, enables the identification of an individual. PII includes but is not limited to a person's:

1. Full name, including legal name and/or preferred name;

2. Social Security Number;

3. Driver's License or other State Identification Number;

4. Passport Number;

5. Biometric information including physiological, biological, or behavioral characteristics, including an individual's DNA, that can be used alone or in combination with other identifying data to establish an individual's identity;

6. Geolocation Data;

7. Internet or network activity, including browsing history, search history, and information regarding an identifiable individual's interaction with an internet website, application, or advertisement;

8. Financial account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account; and

9. Identifiable health information, including disability status, related to the past, present, or future physical or mental health or condition of an individual.

B. "Privacy Rights" includes, but is not limited to, an individual's right to control the use and collection of their Personally Identifiable Information.

C. "Unit Head" means the administrator(s) responsible for a Unit.

III. Applicability

A. This Policy applies to all Personally Identifiable Information (PII), regardless of the relationship an individual may have with the University, including but not limited to current, past, and prospective students, parents, employees, and human research data subjects.

B. This Policy applies regardless of the origin of the PII, including but not limited to existing UMD data sets, new UMD-collected data, and data sets received from or created by third parties.

C. This Policy applies to all members of the University community, visitors to the University, and users of University information systems with access to PII, including but not limited to students, faculty, staff, Unit Heads, and third-parties. All members of the university community who have access to PII must adhere to this policy and related standards and guidelines.

D. This Policy also applies to all locations and operations of the University including but not limited to applications, projects, systems, or services that seek to access, collect, or otherwise use PII.

IV. Policy

A. Principles

The following principles will guide the University and its units when making decisions on the collection or use of PII that may impact an individual's Privacy Rights. These principles provide a framework based upon respect, equity, transparency, responsibility, and limitations. It is the University's intent to use proportionate and effective measures to ensure that the University and the campus community will protect and respect an individual's Privacy Rights within the framework and limitations of applicable law and applicable policies.

1. RESPECT: The collection, use, and storage of PII will be balanced with the interests of impacted individuals. Privacy risks, including an individual's rights, dignity, and expectation of privacy, must be considered prior to such collection, use, or storage.

2. EQUITY: The educational and work environment should be one rich in diversity, inclusive, and supportive of all members of the campus community. Collection and use of PII will be consistent with the furtherance of these values.

3. TRANSPARENCY: Information regarding the collection, use, and storage of PII will be made available to individuals upon request. Individuals will have the ability to discover the purpose for which their data is used.

4. RESPONSIBILITY: The collection, use, and storage of PII involves risk, including but not limited to risks related to the appropriate collection of data, use of data, security of data, sharing of data, and data ownership. University activities must be proactively reviewed to ensure that such risks are understood and mitigated.

5. LIMITATION: PII that is collected, stored, and used will be limited to information that is relevant to accomplish clearly defined outcomes that support the University's mission. (e.g., legitimate educational, research, public service, or administrative purposes). PII will be securely deleted when no longer needed, subject to the University's Records Retention Schedule (https://purchase.umd.edu/administrative-services/records-retention/umd-records-retention-schedule).

B. Expectation of Privacy

1. The University recognizes a reasonable expectation of privacy in the data of its employees, affiliates, and students, in the interest of promoting academic freedom and an open, collegial atmosphere. This expectation of privacy is subject to applicable state and federal laws in addition to University policies and regulations, including the Principles set forth in this Policy, the University's Policy on Acceptable Use of Information Technology Resources, and all associated standards and guidelines.

2. Some PII may be subject to disclosure under the Maryland Public Information Act.

3. The University Reserves the right to access and use PII in its sole discretion to investigate actual or suspected instances of misconduct or risk to the University, students, faculty, staff, and third parties, subject to applicable law, University policy, and associated standards and guidelines.

C. Regulatory Obligations and Interpretations

1. As referenced above, the University must comply with Federal, State, and/or local laws and regulations related to privacy. This Policy and its associated Standards and Guidelines establish a framework for the University's compliance with privacy-related regulations. This framework governs the University's implementation of regulation-specific policies and standards, to address the collection and use of PII in compliance with structures including, but not limited to the Health Information Portability & Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulation (GDPR), and Maryland's Protection of Personally Identifiable Information by Public Institutions of Higher Education law.

V. Implementation

A. This Policy, the associated Privacy Standards and Guidelines, and the implementation of those instruments are overseen by the University's Chief Data Privacy Officer (umd-privacy@umd.edu).

B. The Division of Information Technology (DIT) is responsible for supporting Units with the implementation of this Policy by providing effective tools, appropriate resources, and training in order to meet the guidelines and standards of the Privacy Policy while minimizing potential costs and workload burdens imposed on Units.

C. Standards and Guidelines

1. This Policy is supplemented by Privacy Standards and Guidelines that are developed in coordination with appropriate stakeholders and the University IT Council and maintained by the Chief Data Privacy Officer. These Standards and Guidelines address the operationalization of the privacy Principles identified in Section IV.A, including but not limited to access to specified data types, vendor engagement, incident response, and the exceptions process.

2. The Vice President for Information Technology & Chief Information Officer (VPIT & CIO) or designee may issue, amend, or rescind such Privacy Standards and Guidelines as required to comply with legal obligations and University policy.

D. Exceptions

1. Where a legitimate need has been demonstrated, such as a novel use of an existing data set for health and safety purposes, the VPIT & CIO or designee, in consultation with appropriate stakeholders, may grant exceptions to this Policy and its Standards and Guidelines.

2. When considering requests for exceptions, the VPIT & CIO or designee, in consultation with appropriate University stakeholders, will evaluate the documented purpose for the exception and the privacy risks to the individuals affected.

3. Subject to the University's legal obligations or circumstances that necessitate immediate access, the University may provide advance notification to an individual prior to the use of the individual's PII pursuant to an exception request. In certain instances, individuals may be unavailable to receive such advance notification, or such notification may not be reasonably practicable. In such cases use may occur without notification, consistent with applicable law.

VI. Policy Violations

A. Suspected violations of this Policy will undergo a standard University review in accordance with relevant University policies to determine responsibility.

B. University employees or students who are found responsible for violating this Policy and/or the associated Privacy Standards and Guidelines may be subject to disciplinary action in accordance with relevant University policies. Furthermore, certain violations may result in civil penalties and/or criminal prosecution.

C. Unit Heads who are found responsible for knowingly or intentionally violating this Policy and/or the associated Privacy Standards and Guidelines, where such violations lead to, or are responsible for, a reportable security incident or other penalties imposed by government regulators or agencies, may obligate the responsible unit to cover a portion or all of the University remediation costs and/or externally imposed penalties associated with the violation.

Appendix 1

UNIVERSITY SENATE | **CHARGE**

Charged: April 2, 2021 | Deadline: November 5, 2021

Proposal for the Establishment of a University Privacy Policy (Senate Document #20-21-15)

Information Technology (IT) Council | Chair: Derek Richardson

The Senate Executive Committee (SEC) and Senate Chair Dugan request that the Information Technology (IT) Council review the proposal entitled, *Proposal for the Establishment of a University Privacy Policy*.

The IT Council should:

1. Review the *Proposal for the Establishment of a University Privacy Policy*.
2. Review the draft privacy policy included in the proposal.
3. Review the Maryland Higher Education Privacy Act (MD House Bill 1122).
4. Review the University of Maryland Policy on Acceptable Use of Information Technology Resources (X-1.00[A]).
5. Review relevant Division of Information Technology IT Security Standards associated with IT privacy.
6. Review similar privacy policies at Big 10 and other peer institutions to identify best practices and principles.
7. Consult with the Vice President for Information Technology & Chief Information Officer.
8. Consult with the University's Chief Privacy Officer.
9. Consult with various campus stakeholder groups to collect feedback on best practices and principles in privacy policies.
10. Consider what elements should be included in a privacy policy at the University.
11. Consider whether the University of Maryland Policy on Acceptable Use of Information Technology Resources (X-1.00 [A]) aligns with the principles of a separate privacy policy, or whether adjustments are needed.
12. Consult with a representative of the Office of General Counsel on a proposed new policy or changes to existing University policy.
13. Recommend a new privacy policy for the University in alignment with the Maryland Higher Education Privacy Act.
14. If appropriate, recommend revisions to the University of Maryland Policy on Acceptable Use of Information Technology Resources (X-1.00 [A]), in order to align it with the development of a separate privacy policy.

We ask that you submit a report to the Senate Office no later than **November 5, 2021**. If you have questions or need assistance, please contact Reka Montfort in the Senate Office, reka@umd.edu.

Appendix 2

Institution	Has Privacy Policy?	Has supplemental materials (statements, guidelines, standards, etc)?	Policy establishes principles?	Policy establishes expectations of privacy?	Policy "owner"	Link(s)
University of Indiana	Yes	Procedures in Policy	Indirect	Yes	CIO	https://policies.iu.edu/policies/it-07-privacy-it-resources/index.html
Michigan State	Part of AUP	No	No	Indirect	CIO	https://tech.msu.edu/about/guidelines-policies/aup/
Northwestern	Yes	No	Indirect	No	Compliance & Ethics	https://www.it.northwestern.edu/policies/privacy-issues.html
Ohio State	Yes	Yes	Yes	No	CIO	https://it.osu.edu/privacy
Penn State	Yes	Yes	Yes	Yes	CISO	https://policy.psu.edu/policies/ad53
Purdue	Part of security policy	Yes	Indirect	Indirect	CIO	https://www.purdue.edu/policies/information-technology/viib8.html
Rutgers	Only for specific areas (ex., libraries)	N/a	N/a	N/a	N/a	https://www.libraries.rutgers.edu/about-rutgers-university-libraries/policies-and-guidelines/privacy-policy
University of Illinois - Urbana-Champaign	System-level policy	Yes	No	Indirect	State System	https://www.vpaa.uillinois.edu/resources/web_privacy
University of Iowa	Part of AUP	Yes	Indirect	Indirect	CIO	https://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources
University of Michigan	Yes	Yes	Yes	Indirect	CIO	https://umich.edu/about/privacy-statement/
University of Minnesota	MN Law	Yes	N/A	Indirect	CISO	https://privacy.umn.edu/
University of Nebraska-Lincoln	Yes	No	Indirect	Indirect	CIO	https://its.unl.edu/unlprivacypolicy/
University of Wisconsin - Madison	Yes	No	Indirect	Indirect	Area-specific	https://www.wisc.edu/privacy-notice/