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.

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 (PII)" 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;
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 related to the past, present, or future physical or mental health or condition of an individual.

III. Applicability

A. This Policy applies to all 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, 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 business decisions 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 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. 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.

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 this Policy, our Acceptable Use Policy, 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. Standards and Guidelines

1. This Policy is supplemented by Privacy Standards and Guidelines that are maintained by the Chief Data Privacy Officer. These Standards and Guidelines address the operationalization of the University's privacy principles, including but not limited to access to specified data types, vendor engagement, and incident response.

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, or to meet the needs of the University Community.

3. The current Privacy Standards and Guidelines can be found at: [[insert hyperlink]]

C. Exceptions

1. Where a legitimate need has been demonstrated (e.g., academic integrity investigations), the VPIT & CIO or designee, in consultation with appropriate stakeholders, may grant exceptions to this Policy and its Standards and Guidelines. The exceptions process can be found at: [[insert hyperlink]]

2. When considering requests for exceptions, the VPIT & CIO or designee, in consultation with appropriate University stakeholders, will evaluate the documented business 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 providing access to the individual's PII pursuant to an exception request. In certain instances, an individual may be unavailable to receive such advance notification, or such notification may not be reasonably practicable. In such cases access may be permitted without notification, consistent with applicable law.

VI. Policy Violations

A. Policy violations that result in, lead to, or are responsible for a reportable security incident or other penalties imposed by government regulators or agencies may result in the responsible unit being required to cover all University costs and/or government penalties associated with the violation.

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.


UPDATE ON UMD'S PRIVACY POLICY

WHAT IS PRIVACY?

Personal Privacy

- The right to be left alone, or freedom from interference or intrusion.
- The right to have some control over how your personal information is collected and used.

Organizational Privacy

- The duty to respect an individual's personal privacy.
- Organizational Privacy programs ensure the appropriate collection and use of an individual's information.

PRIVACY POLICY AT UMD

UMD does not have a Privacy Policy

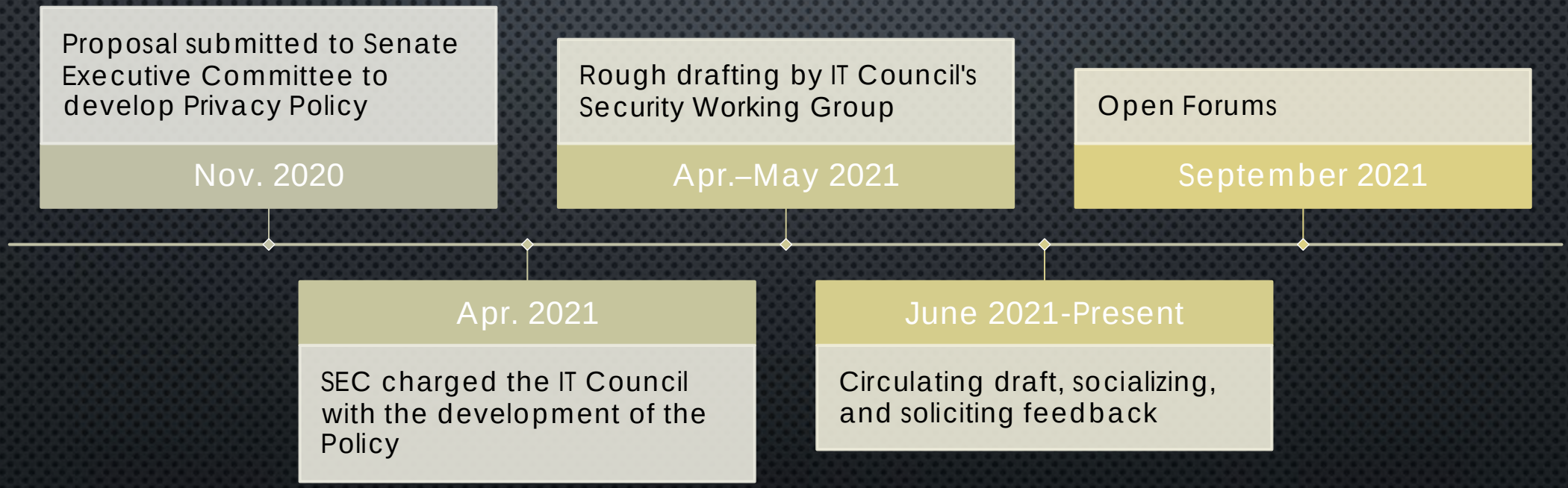
From UMD's Acceptable Use Policy:

- "To the extent possible in the electronic environment and in a public setting, a user’s privacy will be preserved."

WHAT ARE WE MISSING?

- Articulated principles
- Expectations
- Implementation process
- Rules for exceptions
- Consequences for violations

TIMELINE: WHAT'S HAPPENED SO FAR



BENCHMARKING: WHERE IS UMD COMPARED TO ITS BIG10 PEERS?

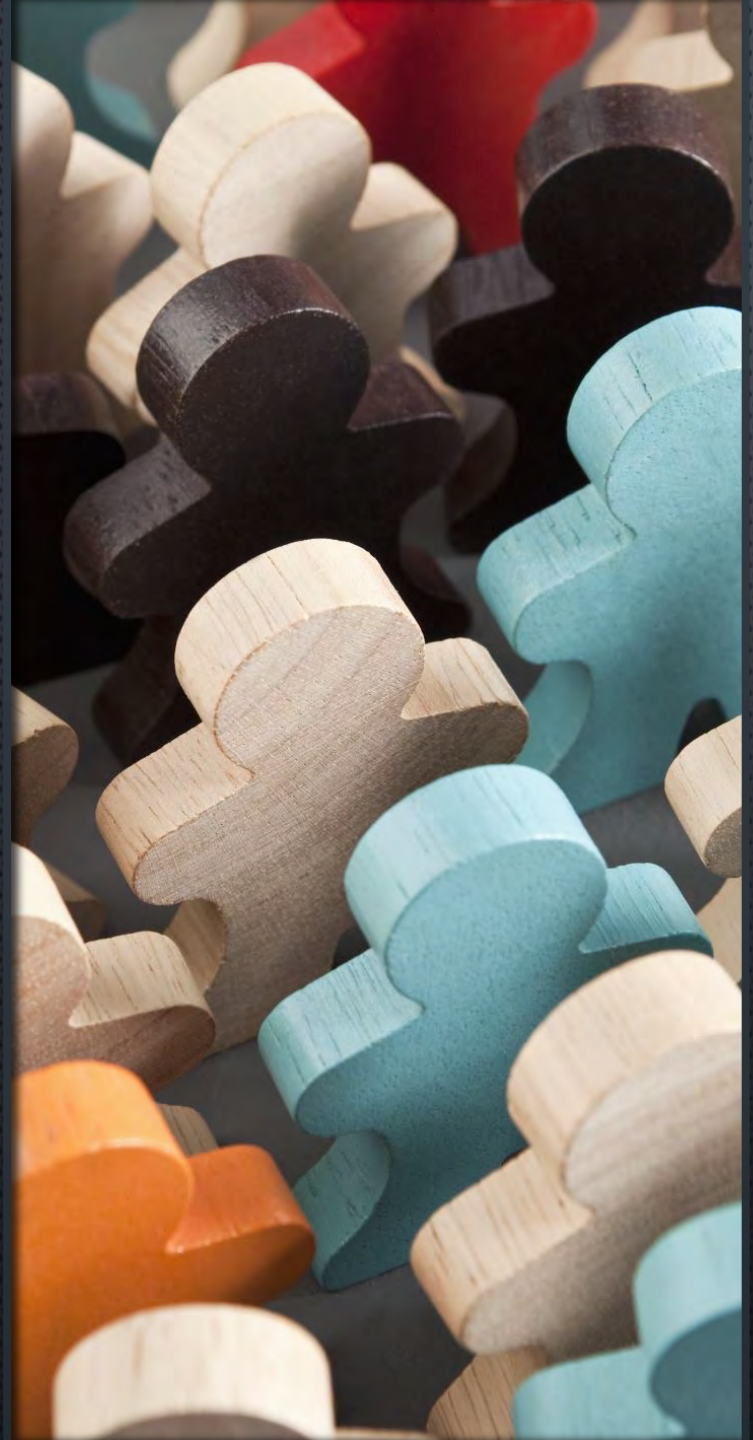
- 7 institutions in the Big Ten Academic Alliance have Indivdual/Direct Privacy Policies
- Of the remaining institutions, 4 incorporate their Privacy Policy into other Policies (2 in the Acceptable Use Policy, 1 in the Security Policy, and 1 in a system-level policy)
- Only 1 school does not have an enterprise-level policy that governs privacy

PRIVACY PRINCIPLES

- Respect
- Equity
- Transparency
- Responsibility
- Limitation

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.



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.

TRANSPARENCY

- Information on the collection, use, and storage of PII will be made available to individuals. Individuals will have the ability to discover the purpose for which their data is used.

RESPONSIBILITY

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

LIMITATION

- PII THAT IS COLLECTED, STORED, AND USED WILL BE LIMITED TO INFORMATION THAT IS RELEVANT TO ACCOMPLISH CLEARLY DEFINED OUTCOMES THAT SUPPORT LEGITIMATE EDUCATIONAL, RESEARCH, PUBLIC SERVICE, OR ADMINISTRATIVE PURPOSES. PII WILL BE SECURELY DELETED WHEN NO LONGER NEEDED, SUBJECT TO ANY UNIVERSITY RECORDS RETENTION REQUIREMENTS.

EXPECTATION OF PRIVACY

- A reasonable expectation of privacy
- Subject to regulatory and University Obligations (Ex. Maryland Public Information Act)
- Misconduct Investigations
- Cybersecurity

STANDARDS

- Turning Principles into Action
- Making Privacy work
- Built by the Community

EXCEPTIONS

Exceptions granted based on a process involving many stakeholders

- Consistent Criteria
- Transparent
- Documented/Recorded

Examples of exceptions:

- COVID Compliance

Policy Violations

- Where applied to individuals:
  - Exact same process as other violations of university policy
- Where applied to units:
  - New at UMD
  - Unit may have to pay some of cost for a breach or fine
- Example of Unit Policy Violation:
  - Collecting/using Social Security Numbers to match identities

WHAT'S NEXT?

- Send questions/comments/concerns to:
  - jgridley@umd.edu
  - umd-privacy@umd.edu
- Final presentation for vote at December Senate session
- Development of Standards to begin Spring 2022