University of Pittsburgh
Privacy Policy Committee Charter

I. Preamble

This body is called the Privacy Policy Committee ("Committee"). It is authorized by the Chancellor and will serve at the Chancellor's discretion. The Chancellor has authorized the Senior Vice Chancellor and Chief Legal Officer ("SVC-CLO"), or their designee, to direct the operations of this Committee, consistent with the terms of this Charter. This Charter outlines the purpose, relevant background, scope, responsibilities, composition, and operations of the Committee, as well as the review process for any proposals generated by this Committee.

This document should be read in conjunction with Policy AO 01, Establishing University Policies, and all other applicable University policies, protocols, and procedures.

II. Purpose

This Committee is created for the purpose of proposing a new University Policy, as well as documents that support its implementation, which will govern how the University safeguards the privacy of non-public protected information in its records and will establish the framework for compliance with applicable statutory and regulatory requirements.

III. Background

While the University has other privacy related policies in place, including Policy CS 30 which governs the responsibilities of the University and its employees who handle protected health information, and Policy AC 04 which governs the obligation to protect students' rights to access their Education Records, there currently is not a University-level Policy that defines categories of regulated data, explains privacy roles across the University, or provides guidance for decision-making associated with the collection and disclosure of non-public and potentially private information. Furthermore, as part of its efforts to improve its data privacy program, the University identified the need for a policy that articulates and defines the appropriate safeguards for the collection, storage, and purging of sensitive data at the University as well as establishes effective data management controls.

Additionally, the University identified the need for clarifying the University Privacy Officer's role to oversee privacy matters; establishing principles to govern a privacy program, which includes privacy impact assessments; clarifying privacy oversight responsibilities (e.g., Office of Compliance, Investigations, and Ethics ("CIE Office"), Human Resources, and Pitt IT); and

establishing training requirements related to privacy practices and policies at the University that would be required for certain University members.

To this end, the Committee is charged with proposing a University-level Policy that would formally establish the University's framework for compliance and responsibility regarding privacy and the protection of an individual's personal information as required by various laws and regulations.

IV. Scope and Authority

The Committee will recommend a new University Policy, and its supporting documents (e.g., procedures and standards), to govern safeguarding the privacy of non-public protected information. In doing so, the Committee's deliberations must address the following topics:

- **Scope**. Identify and clearly define the type of non-public protected information covered by the Policy;

- **Compliance**. Address all relevant laws and regulations, including those governing regulated data such as Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Social Security Numbers (SSNs), Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR), and other international regulations;

- **Align.** Review other relevant University policies governing regulated data, such as those covered by FERPA and HIPAA, as well as those governing information security, and ensure the proposed Policy aligns with those existing University policies;

- **Procedures, Standards, and Guidelines.** Develop necessary procedures, standards, and guidelines (e.g., confidentiality, record keeping) for the collection and disclosure of non-public protected data, including setting forth individual rights and protections associated with personal information; storage and disposal of data; and conducting privacy impact assessments to evaluate associated risk(s), including risks associated with third party disclosures;

- **Roles and Responsibilities.** Establish roles and responsibilities of various offices and departments (e.g., CIE Office, Human Resources, Pitt IT) as they relate to privacy management and a privacy program.

- **Privacy Officer.** Articulate and describe the role and responsibilities of the University Privacy Officer, including the position's oversight authority; and

- **Privacy Program.** Establish principles and address key components that will be used to formally establish the University's Privacy Program. Key components to be addressed by the proposed Policy include data/privacy risk assessments and privacy

impact assessments; privacy by design; regular training for University members; privacy due diligence associated with third-parties; maintenance and regular review of security controls and the University's data incident response plan; and regular auditing of the Privacy Program.

V. Responsibilities

As provided above, the Committee is created to propose a Policy to govern safeguarding the privacy of non-public protected information at the University. To perform this function, the Committee has the responsibility to:

- Review the University's current privacy management practices and support services;
- Review existing University policies that speak to protected information, including Policy CS 30 and Policy AC 04, and consult with other University policy committees currently drafting policies concerning related privacy matters, such as data management and security;
- Discuss best practices in higher education related to safeguarding the privacy of non-public protected information, including benchmarking peer universities' respective policies on the matter;
- In accordance with the terms of this Charter, consult with the Information Technology Advisory Committee (ITAC) and University stakeholders (including departments, schools, faculty, staff, and students) who have a role in safeguarding the management of non-public information to inform the drafting of the proposed Policy;
- Incorporate or address applicable local, state, federal, and international requirements into the proposed Policy and associated procedures;
- Consistent with the terms of this Charter, discuss proposed requirements and responsibilities with interested stakeholders in the University community, including representatives from each of the Regional Campuses
- Recommend a draft Policy for review pursuant to the process described in Section VII below, and consider feedback during that review; and
- Recommend accompanying draft procedures or other supplemental material needed for the effective and efficient implementation of the proposed Policy.

It is expected that the Committee will work in confidence to have a full and frank discussion of all options. Individual members should maintain the deliberations of the Committee confidential and are expected to not discuss the content of the Committee's deliberations outside of the Committee, unless authorized to do so by the Committee. The broader community will have an opportunity to consider the Committee's proposals pursuant to the process described in Section VIII below.

VI. Composition

The Committee will be chaired by **Laurel Gift**, Assistant Vice Chancellor for Compliance, Investigations, and Ethics. The Committee will include the following members:

1. **John Duska,** Chief Information Security Officer
2. **Christian Stumpf,** Vice President of Finance and Administration, University of Pittsburgh Johnstown, Regional Campus Representative
3. **Jeff Whitehead,** Executive Director of Global Engagement
4. **Aynsley Jimenez,** Compliance Manager, Office of Human Resources
5. **Mark Anderson,** Executive Director for Risk Management
6. **Jonathan Helm,** University Registrar
7. **Bill Yates,** Vice Chancellor for Research Protections
8. **Uduak Ndoh,** Vice Chancellor and Deputy Chief Information Officer, Health Sciences
9. **Ken Fish,** Associate Professor of Psychiatry, Senate Computing and Information Technology Committee (SCITC) Representative
10. **Devon Batty,** Student Government Board Judicial Committee Vice-Chair
11. **Carolyn Hoyt**, VC of Advancement Operations & Chief PAE Strategy Officer
12. **Sharon Joyner,** Staff Council Representative

Brittany Conner will help facilitate and support the work of the Committee on behalf of the Office of Policy Development and Management.

Andrew Eisman will support the work of the Committee on behalf of the Office of University Counsel.

Ericha Geppert will support the work of the Committee on behalf of the Office of Compliance, Investigations, and Ethics.

VII. Operations

The Committee will meet monthly, or more frequently as circumstances dictate. The Committee's proposed Policy on Privacy will be submitted to the SVC-CLO, or their designee, no later than the 2023-24 Academic Year. The SVC-CLO may ask for interim status reports.

After the SVC-CLO's, or their designee's, review is complete, the draft Policy will be submitted to the Office of Policy Development and Management ("Policy Office") to coordinate its review consistent with Policy AO 01.

VIII. Proposed Policy Review Process

The review process for the Committee's recommended Policy is as follows:

- University comment period;
- Academic Leadership Team;
- University Senate's Committee(s) on Computing and Information Technology Committee (SCITC)
- Faculty Assembly;
- University Senate Council; and
- Administrative Leadership.

The Committee will coordinate with the Policy Office to consider feedback provided throughout this process.

Once this review process is complete, the proposed Policy will be sent to the Policy Office for review and submission to the Chancellor in accordance with Policy AO 01.

IX. Amendment

Any amendments to this Charter must be made in accordance with Policy AO 01 and receive the approval of the Chancellor or designee.

This Committee shall expire on the publication of a new University Policy that governs Privacy, unless otherwise directed by the Chancellor.