**Personally Identifiable Information Policy**

**Policy**

Members of the University community shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it. All individuals who dispense, receive, and store PII have responsibilities to safeguard it.

In adopting this policy, the University is guided by the following objectives:

1. To enhance individual privacy for members of the University community through the secure handling of PII;
2. To ensure that all members of the University community understand their obligations and individual responsibilities under this policy by providing appropriate training that will permit the University community to comply with both the letter and the spirit of all applicable privacy legislation;
3. To increase security and management of PII by:
	1. establishing broad awareness of the confidential nature of PII;
	2. a consistent policy about the use of PII throughout the University; and
	3. ensuring that access to SSNs and other PII for the purpose of conducting University business is granted only to the extent necessary to accomplish a given task or purpose.
4. To use, throughout the University, a unique University ID (DoaneID) that serves as the primary identification element for persons associated with Doane University and is applicable across the entire institution, reducing reliance on the SSN for identification purposes.
5. To not transmit, process, or store any complete credit card data on any University owned/controlled computers, servers, desktops, laptops, disks, flash drives, or other portable or mobile devices.

Managers and designated staff are responsible for oversight of personally identifiable information in their respective areas of University operations

**Purpose of this Policy**

Doane University creates, collects, maintains, uses, and transmits personally identifiable information relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, and staff. The University is committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations in order to maximize trust and integrity.

**Scope of this Policy**

This policy applies to all members of the University community, including all full- and part-time employees, faculty, students and their parents or guardians, and other individuals such as contractors, consultants, other agents of the community, alumni, and affiliates that are associated with the University or whose work gives them custodial responsibilities for PII.

**Policy Definitions**

**Minimum Necessary**: *Minimum Necessary* is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.

**Personally Identifiable Information (PII)**: Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, name, etc.

**Personal Identifier (PID)**: A PID, a sub-category of PII, is a unique code assigned to or utilized by an individual to identify that individual. PIDs are used primarily, but not exclusively, for the purpose of electronic operations. The Doane UserID and Doane Gmail Address are examples of PIDs.

**Policy Requirements**

1. **Data Stewards**

The following are the Data stewards who will administer this policy in their respective areas of University operations. They will resolve the responsibility for the data, if any data elements overlap more than one area.

* 1. Vice President for Institutional Advancement: Alumni and donors
	2. Vice President for Enrollment and Marketing, and Director of Financial Aid: Prospective students and applicants
	3. Vice President for Academic Affairs, and Registrar: Students (academic records) Faculty, Visiting Scholars, Graduate/Research/Teaching Assistants, and research staff
	4. Vice President for Student Leadership (Student Leadership)
	5. Director of Human Resources: Administrators, staff, service employees and prospective employees
	6. Public Safety Director: Doane ID Card for employees and College of Arts and Sciences students. Physical security of areas containing confidential information.
	7. Vice President for Finance and Administration: Business associates, consultants, contractors, and vendors
	8. Vice President for Information Technology & Chief Information Officer: Issuance of the DoaneID, Doane email address and the security of PII in computer storage and transmission.
1. **Personally Identifiable Information**
	1. PII may be released only on a Minimum Necessary basis and only to those individuals who are authorized to use such information as part of their official University duties, subject to the requirements:
		1. that the PII released is narrowly tailored to a specific business requirement;
		2. that the information is kept secure and used only for the specific official University [business] purposes for which authorization was obtained; and
		3. that the PII is not further disclosed or provided to others without proper authorization as defined above.
	2. PII may be handled by third parties with the strict requirement that the information be kept secure and used only for a specific official authorized business purpose as defined in a Non-Disclosure and Data Use Agreement with that third party.
	3. Exceptions to this policy may be made only upon specific requests approved by the authorized University official responsible for such information as specified in this policy above and only to the degree necessary to achieve the mission and business needs of the University. Any and all exceptions made must be documented, retained securely, and reviewed periodically by the appropriate University official or assigned designee.
	4. Directory PII, as defined by Federal and State law and Doane University policy, will be published following the guidelines defined by the Office of the Vice President for Information Technology and Chief Information Officer for Doane University.
2. **Government-Issued Personal Identifiers**
	1. **Social Security Number**
		1. Provision of Information
			1. Doane University collects SSNs:
				1. when it is required to do so by law;
				2. when no other identifier serves the business purpose; and
				3. when an individual volunteers the SSN as a means of locating or confirming personal records.
			2. In other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.
			3. SSN collection must be approved by the appropriate campus official (see the "Policy" section, above). When an SSN is requested, Doane informs the individual what uses will be made of the SSN and whether the disclosure is voluntary, or, if it is mandatory, by what authority.
		2. Release of SSNs

SSNs will be released by Doane University to persons or entities outside the University only:

* + - 1. as required by law;
			2. when permission is granted by the individual;
			3. when the external entity is acting as the University's authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties
		1. Use, Display, Storage, Retention, and Disposal
			1. SSNs or any portion thereof will not be used by Doane to identify individuals except as required by law or with approval by a University official for a University business purpose.
			2. The release or posting of personal information, such as grades or occupational listings, keyed by the SSN or any portion thereof, is prohibited, as is placement of the SSN in files with unrestricted access.
			3. SSNs will be transmitted electronically only for business purposes approved by the campus officials responsible for SSN oversight and only through secure mechanisms approved by the Vice President for Information Technology & Chief Information Officer.
			4. The Data Stewards who are responsible for SSNs will oversee the establishment of business rules for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.
	1. **Non-SSN Government-Issued Identifiers**

In the course of its business operations, Doane has access to, collects, and uses non-SSN government-issued identifiers such as driver's licenses, passports, Employee Identification Numbers (EIN), and military identification cards, among others. Doane follows the Minimum Necessary standard and strives to safeguard these identifiers.

1. **Doane University-Issued Identifiers**
	1. **Colleague ID Number**
		1. Assignment Eligibility and Issuance
			1. The PID (DoaneID) is a unique numeric identifier assigned by the University to any member of the University community who requires an identifying number in any University system or record.
			2. A PID is assigned at the earliest possible point of contact between the individual and the University.
			3. The PID is associated permanently and uniquely with the individual to whom it is assigned.
		2. Use, Display, Storage, Retention, and Disposal
			1. The PID is to be used only for appropriate business purposes in support of University operations.
			2. The PID is used to identify, track, and serve individuals across all University electronic and paper data systems, applications, and business processes throughout the span of an individual's association with the University and presence in the University's systems or records.
			3. The PID is not to be disclosed or displayed publicly by the University, nor to be posted on University electronic information or data systems unless the PID is protected by access controls that limit access to properly authorized individuals.
			4. The PID is displayed and encoded on the official University photo identification card known as the Doane ID Card. The Doane ID Card is the principal means of physical identification at the University, and the use of the Doane ID Card by the cardholder, whether by physical display or when swiped at an electronic reader, will constitute a voluntary disclosure of the PID. Note: Students in the College of Professional Studies and College of Education do not have physical ID Cards.
	2. **DoaneID**
		1. Assignment Eligibility and Issuance
			1. The DoaneID is a unique numeric assigned by the University to an individual.
			2. The DoaneID is assigned to all persons who may require access to electronic services at the University, including students, faculty, alumni, administrators, staff, service employees, and other individuals (such as contractors, consultants, and affiliates) associated with the University.
			3. The DoaneID is permanently and uniquely associated with the individual to whom it is assigned.
			4. The DoaneID, alone, without a password, will not be used for access to Doane’s electronic network.
		2. Use, Display, Storage, Retention, and Disposal
			1. The DoaneID is used, in conjunction with an individually set password, as an authenticated identifier for online transactions and may be used, in addition to the PID, to identify and track individuals within the University systems, applications, and business processes.
			2. Each member of the University community will be held fully responsible for any activity authorized by that individual's DoaneID and password.
			3. Under the Family Educational Rights and Privacy Act (FERPA), the DoaneID may be used as directory information as long as the identifier cannot be used standing alone (i.e., without a password) by unauthorized individuals to obtain sensitive, non-public (i.e., non-directory) information about an individual from education records.
			4. The release or posting of personal information keyed by the DoaneID, such as grades, is prohibited.
	3. **Local User ID Numbers**

In addition to University Identification Numbers (PIDs) and DoaneIDs, Doane University colleges, divisions and departments may issue other system-unique identifiers. Doane University follows the Minimum Necessary standard and strives to safeguard these identifiers.

1. **Other Externally-Assigned Identifiers and Other Personally Identifiable Information**

Doane University has access to, collects, and uses various externally-assigned identifiers other than those indicated above in the course of its business operations. These identifiers include, but are not limited to credit and debit card numbers and bank account numbers. Doane uses third party vendors to manage PCI data and no PCI data is stored by Doane or on Doane equipment. Doane University follows the Minimum Necessary standard and strives to safeguard these identifiers.

1. **Responsibility for Maintenance and Access Control**
	1. DoaneID’s and email addresses are maintained and administered by Doane University Information Technology Services (ITS).
	2. Access to electronic and physical repositories containing SSNs, PIDs, and DoaneIDs will be controlled based upon reasonable and appropriate administrative, physical, technical, and organizational safeguards.
	3. Individuals who inadvertently gain access to a file or database that contains SSNs or PIDs for which they have not been authorized shall report it immediately to the Vice President for Information Technology & Chief Information Officer.
2. **Enforcement**

Violations of this policy are subject to action by the University. Violations will be referred to the Vice President for Information Technology & CIO, who will report issues and problems for review by the appropriate Administrator or the Dean of Student Leadership and the Academic Dean, and will be referred to the appropriate administrative or judicial proceedings. Violators may be billed or fined for unethical or illegal use of information technology. They may also be subject to dismissal, suspension, loss of network and computing privileges, and/or legally prosecuted.