COLLEGE of CHARLESTON

OFFICIAL POLICY

10.30	Data Classification Policy	6/18/2025

Policy Statement

Information is a valuable resource at the College of Charleston, requiring responsible management by all College of Charleston community members. This policy outlines the classification schema for institutional data.

Policy Manager and Responsible Department or Office

Office of the Chief Information Officer

Departments/Offices Affected by the Policy

All College of Charleston Departments and Offices

Policy: Data Ownership

The College of Charleston owns administrative data. As such, all members of the College community have the obligation to appropriately use and safeguard the asset in all formats and locations.

Intellectual Property data –please refer to the College's intellectual property policy for information on data ownership.

Data Management Schema

Data Trustees

Data trustees are CofC executives who have overall responsibility for all the data sets maintained by the units reporting to them. Institutional data trustees consist of the Provost, other Vice-Presidents and the Chief Information Officer (CIO). Individually, the data trustees are accountable for all the data sets within their division. The CIO has the additional responsibility for ensuring an adequate and appropriate technical infrastructure is in place to support the data needs of the institution across all divisions.

The data trustees are responsible for ensuring that campus **institutional data** resources are used in ways consistent with the mission of the College of Charleston. The data trustees have the responsibility for the appointment and accountability of data stewards.

Data Stewards

Data stewards, designated by the data trustees, are senior level officials who have planning and policy responsibilities for data in their functional areas. Data stewards, or their designees, are responsible for recommending policies, and establishing procedures and guidelines concerning

the accuracy, privacy and integrity of the data subsets for which they are responsible. Individually, data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas.

They have overall responsibility for the data in the subsets overseen by all their designated data managers.

Data Managers

Data managers, designated by the data stewards, are generally operational managers within a functional area overseeing the data for a particular subject area. Data managers have day-to-day responsibility for managing administrative processes and establishing business rules for the transactional systems. They have operational responsibility for the data management activities related to the collection, maintenance, protection, and dissemination of data in their functional areas.

The data manager may authorize operational tasks to be performed by data users outside the units that report to the data manager. The data managers are accountable for the data subsets they manage, whether the data are collected or maintained directly by the data manager (or their staff), by data users in other units or by external sources.

Data Users

Data users are CofC employees who have been granted authorization by the data managers to access institutional data. Authorization is granted for a specific level of access, as defined by the data management policies, solely for the conduct of institutional business.

Data Classifications

By default, all **institutional data** will be designated as internal data for use within College of Charleston or to satisfy institutional external reporting requirements to state agencies, CHE, federal, or other external agencies. College of Charleston employees will have access to these data for use in conducting College of Charleston business. The permission to view or query **institutional data** should be granted to all data users for all legitimate institutional purposes. As part of the data definition process, data stewards will assign each data element and each data view in institutional data to one of four classifications: Public, Internal Use, Confidential, or Restricted.

NOTE: In all data classifications, users with a "need to know" to perform their job duties will have access to the appropriate information but will require additional authentication and authorization requirements (i.e., two-factor-no SMS/TXT, three-factor, and/or biometric authentication)

In some circumstances, confidential and restricted data may be classified as institutional if specific identifying data elements are removed (de-identified).

All College of Charleston information is categorized into four main classifications:

Public Data

Institutional data that have no access restrictions are available to the general public. These data will be designated as unrestricted or public data.

1. Example: Information on the public website

Internal Use Data

Information used in the College's daily operations that is not confidential or legally protected but should not be made public and should only be disclosed under limited circumstances. Other users must be granted specific authorization by the data owner or data steward to access the data since the data's unauthorized disclosure, alteration, or destruction may cause perceivable damage to the institution.

Examples of internal use data elements:

1. Work phone numbers, policies, procedures, and standard interagency communications.
2. All information identifiable to an individual (including students, staff, faculty, trustees, donors, and alumni) including but not limited to dates of birth, driver's license numbers, employee and student id numbers, position descriptions and license plate numbers.
3. The University's proprietary information including but not limited to intellectual research findings, intellectual property, financial data, and donor and funding sources.

Confidential Data

Confidential data are data that, if disclosed to unauthorized individuals, could significantly harm the organization, its stakeholders, or individuals. This data type requires stringent protection measures to ensure its confidentiality, integrity, and availability.

Examples of confidential data elements:

1. Personally identifiable information (PII).
2. Information related to law enforcement.
3. Information related to minors.
4. Business-critical information such as trade secrets, strategic plans, and proprietary methodologies.
5. Sensitive employee information includes performance reviews, salary details, and disciplinary records.
6. Information security plans.

Restricted Data

Institutional data for which there is a legal obligation not to disclose. Restricted data are susceptible information that, if disclosed, modified, or destroyed without authorization, could cause severe harm to the organization, its stakeholders, or individuals. This data classification mandates the highest security controls and access restrictions to prevent unauthorized access and ensure data integrity.

Highly sensitive information in use by the College and is protected by statutory penalties if disclosed in an unauthorized manner.

Examples of restricted data elements:

1. All regulated data
2. Family Educational Rights and Privacy Act of 1974 (FERPA);

a. FERPA protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

1) **Academic Information:** Grades, transcripts, class lists, student course schedules, and academic performance records.
2) **Personal Information:** Student's name, identification number, social security number, and other personal identifiers.
3) **Enrollment Records:** Documents related to student enrollment, attendance, and participation in educational activities.
4) **Disciplinary Records:** Information related to student conduct, disciplinary actions, and behavior incidents.
5) **Health Records:** Medical and health information maintained by the school, such as immunization records and records of visits to the school nurse.
6) **Special Education Records:** Documents related to special education services, including Individualized Education Programs (IEPs).

3. Payment Card Industry (PCI) information such as Credit card or debt card number in combination with any required security code. Card verification value information.
4. Gramm-Leach-Bliley Act (GLBA) provides limited privacy protections for private financial information. Additionally, the GLBA codifies protections against the practice of obtaining personal information through false pretenses. GLBA implements rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information.

Procedures Related to the Policy

All **institutional data** will be classified according to the structure established by this policy. It will be classified and used with appropriate and relevant levels of access and sufficient assurance of its security and integrity in compliance with existing laws, rules, and regulations.

Related Policies, Documents, or Forms

1. Intellectual Property - **http://policy.College of Charleston.edu/documents/9.1.13.pdf**
2. Data Dictionary Procedures - TBD
3. Access Control Policy - TBD
4. Data Principles – **https://charleston.edu/policy/documents/cofc-data-principles-final.pdf**
5. Electronic Communications - **http://policy.College of Charleston.edu/documents/10.14.pdf**
6. Data retention and Destruction College Policies - **11.4 Retention and Destruction of Records**
7. Media Disposal - **https://admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf**
8. Incident Response - **http://it.College of Charleston.edu/security/security-incident-reporting/index.php**
9. Acceptable Use - **http://policy.College of Charleston.edu/documents/10.20.pdf**
10. Data Loss Prevention - **http://policy.College of Charleston.edu/documents/10.19.pdf**
11. SC Privacy Office Data Classification Schema – **https://admin.sc.gov/files/DataClassificationSchemaAndGuidelines071417.pdf**
12. Breach of State Agency Data - **http://www.scstatehouse.gov/code/t01c011.php**

13. **Children's Online Privacy Protection Act (COPPA)**
    Children's Online Privacy Protection Act of 1998 — Regulates the collection and use of children's information by commercial website operators.
    http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=16:1.0.1.3.36
14. **Family Educational Rights and Privacy Act (FERPA)**
    Family Educational Rights and Privacy Act — Protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
    http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33
    http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
15. **Freedom of Information Act (FOIA)**
    Freedom of Information Act — Provides the public with the right, and a process, by which to request access to records from any federal agency (with nine exceptions, such as personal privacy, national security, and law enforcement).
    https://foiaonline.regulations.gov/foia/action/public/home
16. **Gramm-Leach-Bliley Act (GLBA)**
    Gramm-Leach-Bliley Act — Requires financial institutions, which offer products to consumers, to explain their information sharing practices to their customers and to safeguard sensitive data.
    https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act
17. **Privacy Act of 1974**
    Privacy Act of 1974 — Protects the rights of individuals regarding the collection, maintenance, use and dissemination of their information that is maintained in systems of records by federal agencies.
    http://www.justice.gov/opcl/privacy-act-1974
18. **Payment Card Industry Data Security Standard (PCI-DSS)**
    Payment Card Industry Data Security Standard (PCI-DSS) — Sets requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. The law applies to any organization with customers who pay them directly using a credit card or debit card.
    https://www.pcisecuritystandards.org/
19. **U.S. Department of Education — Privacy Technical Assistance Center (PTAC)**
20. The U.S. Department of Education established the PTAC as a resource regarding FERPA and data privacy, confidentiality and security practices. It includes documents, videos, webinars, and other tools, resources, and opportunities to receive assistance to improve privacy, security, and confidentiality of student data systems. These resources are intended to promote compliance with FERPA and other best practices.
21. http://ptac.ed.gov
22. **South Carolina Department of Archives and History**
    One of the missions of the South Carolina Department of Archives and History is to work with state agency and local government officials in the proper management of their records.
    http://rm.sc.gov/Pages/default.aspx

Issue Date: 6/18/2025 **Date of Policy Revision:**	**Next Review:** 6/18/2028

Policy Approval

Policy Number: 10.30 (Data Classifications Policy)

President _____ **Date:** 6/18/25