



OFFICIAL POLICY

11.1	Privacy Policy	04/16/19
------	----------------	----------

**Policy Statement**

The College of Charleston (“the College”) is committed to maintaining the privacy, integrity, security and availability of confidential information created, received, maintained and/or stored by the College, regardless of form.

**Policy Manager and Responsible Department or Office**

Office of Legal Affairs, Office of Human Resources, Division of Information Technology

**Policy**

**I. Purpose and Scope**

This Policy explains the obligations of all members of the College community to protect non-public information and records from unauthorized use or disclosure. It is designed to address applicable federal and state law governing privacy and confidentiality of information, as well as any applicable international privacy regulations.

Everyone with access to College Information and Records must comply with this Policy, including without limitation, students, faculty, staff, alumni, volunteers, contractors, vendors, consultants and other third-parties. It protects all proprietary and non-public information acquired by way of one’s relationship with the College, regardless of how it is stored or recorded. Student information is also governed by College FERPA policies relating to student records.

This Policy covers all “**Confidential Information**,” which means information that is obtained by way of one’s relationship with the College that is not a matter of public record or public knowledge. It includes, without limitation, personal information; College business and financial data, proprietary information and trade secrets; and any other information for which access, use, or disclosure is restricted by any applicable law, regulation or College policy. Confidential Information that is created, documented, received, maintained and/or stored for College business, regardless of its form, is a “**Record**” covered by this Policy. If uncertainty exists about whether something is covered by this Policy, users should treat the item(s) as private and confidential, until directed otherwise by the Office of Legal Affairs and/or appropriate College official.

**II. Use of Confidential Information and Records**

The College limits collection and use of Confidential Information and Records to that required by and necessary to fulfill legitimate College purposes. The College prohibits selling, renting, giving away, loaning or otherwise disclosing any collected or stored personally identifiable information to

any third party for commercial purposes. The College may use or share Confidential Information internally or with third-parties, for authorized College purposes, such as: to provide and improve College services or communications to stakeholders and users; where necessary or appropriate as required by law; to prevent or address fraud, security or technical issues; or to protect the rights, property or safety of the College and its users.

Confidential Information and Records must never be accessed or disclosed without authorization, and all questions about applicable law must be directed to the Office of Legal Affairs. Those with access must maintain Confidential Information and Records as confidential, unless authorized by an appropriate College official. Confidential Information and Records also must be maintained and secured according to these principles:

- A. Confidential Information and Records are to be accessed, used and disclosed only with explicit authorization, in accordance with applicable law, and on a need-to-know basis related to a College function. Such information must never be disclosed outside of the College without express authorization.
- B. Records must be maintained and disposed of according to the College's Policies on Retention and Destruction of Records, South Carolina records retention schedule and accompanying procedures, and any applicable law or regulation.
- C. Records may only be received, maintained, accessed or transmitted on College resources in accordance with the requirements and safeguards of the College's Acceptable Use and other applicable policies.
- D. All users must safeguard any physical key, ID card or computer, network account or password that enables access to Confidential Information and Records.
- E. Upon conclusion of employment or service with the College, all originals and copies of Confidential Information and Records, regardless of form, must be returned to the College and all access to and use of such information shall cease.
- F. Information that the College collects may be subject to disclosure under the South Carolina Freedom of Information Act ("FOIA") unless exempt; thus, all FOIA requests shall be directed immediately to the Office of Legal Affairs and processed under the FOIA Request Policy.
- G. Hiring units are responsible for informing individuals who work or volunteer for the unit of their specific responsibilities under this Policy and related procedures.
- H. Any known or suspected misuse or inappropriate disclosure of Confidential Information or Records should be reported immediately to a supervisor, the Department of Information Assurance and Privacy and/or the Office of Legal Affairs.

### **III. State of South Carolina Data Standards**

To help users appropriately secure and manage Confidential Information and Records, the College has adopted various Data Standards set by the State of South Carolina, that, among other things, categorize data by sensitivity and risk level and designate roles and responsibilities for data use and management.

#### IV. Policy Violations

Policy violations will be treated seriously. Employee violations may result in discipline, up to and including termination. Students who violate this policy may be terminated and/or disciplined under the Student Code of Conduct. Others may lose the opportunity to contract with, volunteer for, or otherwise provide service to the College. Violations may also result in criminal prosecution and/or civil penalties under applicable laws, including without limitation, the South Carolina Family Privacy Protection Act of 2002, South Carolina Trade Secrets Act and Public Employee Ethics law.

#### V. General Data Protection Regulation (GDPR)

Individuals located in the European Economic Area (European Union, Norway, Liechtenstein, and Iceland), may have additional rights, subject to exceptions, including rights related to access, review, updating, correction, processing, or a request for the deletion of the personal information maintained or stored by the College.

#### VI. Contact Information

Questions about this Policy may be directed to:

Office of Legal Affairs  
[legalaffairs@cofc.edu](mailto:legalaffairs@cofc.edu)

Division of Information Technology  
[privacy@cofc.edu](mailto:privacy@cofc.edu)

---

#### Departments/Offices Affected by the Policy

All College Departments and Offices are affected by this Policy.

---

#### Procedures Related to the Policy

See [Privacy Webpage](http://it.cofc.edu/security/privacy/index.php) (<http://it.cofc.edu/security/privacy/index.php>)

---

#### Related Statutes, Policies, Documents or Forms

See [Privacy Webpage](http://it.cofc.edu/security/privacy/index.php) (<http://it.cofc.edu/security/privacy/index.php>)

**Issue Date: 8/23/16**  
**Date of Policy Revision: 4/16/19**

**Next Review Date: 4/16/24**

#### POLICY APPROVAL

(For use by the Office of the Board of Trustees or the Office of the President)

Policy Number:

President or  
Chairman, Board of Trustees *Stephen C. Osborne*

Date: 4/16/2019