COLLEGE of CHARLESTON

OFFICIAL POLICY

11.1	PRIVACY POLICY AND PROCEDURE ON THE SECURITY OF PROTECTED INFORMATION	8/23/2016

Policy Statement

This Policy and Procedure governs the security and confidentiality of personal information entrusted to the care of College of Charleston ("College") to carry out its mission and to certain other sensitive information that is generated and owned by the College. This Policy and Procedure also establishes the principles and processes by which that information will be maintained and managed.

Policy Manager and Responsible Department or Office

Human Resources, Legal Affairs, Information Technology

Policy

BACKGROUND

This Policy and Procedure governs the security and confidentiality of personal information entrusted to the care of College of Charleston ("College") to carry out its mission and to certain other sensitive information that is generated and owned by the College. This Policy and Procedure also establishes the principles and processes by which that information will be maintained and managed.

PURPOSE

The South Carolina Family Privacy Protection Act provides, in relevant part:

§ 30-2-20. Privacy policies and procedures required of all state entities.

All state agencies, boards, commissions, institutions, departments, and other state entities, by whatever name known, must develop privacy policies and procedures to ensure that the collection of personal information pertaining to citizens of the State is limited to such personal information required by any such agency, board, commission, institution, department, or other state entity and necessary to fulfill a legitimate public purpose.

Implementation and adherence to this Policy and Procedure are necessary to comply with the cited statute and to provide for the protection of sensitive information that is maintained or owned by the College.

The specific purposes of this Policy and Procedure are:

To establish a College-wide approach to information security.
To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks and computer systems.
To define mechanisms to protect the reputation of the College and allow the College to satisfy its legal and ethical responsibilities to others.
To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this Policy and Procedure.
To further reduce the risk of exposure and identity theft when a Social Security Number or other personal identifying information is used by the College as a primary identifier and to provide for the consistent, proper and secure management of such information.

SCOPE

This Policy and Procedure is applicable to all members of the College Community including our faculty, staff, students, visitors and contractors who have access to College records regardless of the medium in which those records are stored or where they are located.

SOUTH CAROLINA FAMILY PRIVACY PROTECTION ACT1

State law requires the College to develop privacy policies and procedures to ensure that the collection of personal information pertaining to citizens of the State is limited to such personal information as may be required by the College to fulfill its public purpose.2

The College is also required, as a state entity, to clearly display its Privacy Policy on its

web page, along with the name and telephone number of the College's designee who is "responsible for administration of the policy."3 This Policy and Procedure will be included, therefore, on the College's web site.

When personal information is authorized to be collected by a College Operating Unit, and when that information is subject to disclosure under the Freedom of Information Act4, the operating Unit must, at the time of collection, advise the citizen to whom the information pertains that the information is subject to public scrutiny or release under the Freedom of Information Act. Forms that may be used for such purpose are attached hereto and marked as Appendix A.

1.0 DEFINITIONS5

In this Policy and Procedure the following terms are given the meaning ascribed next to each:

"College Operating Unit" of "Unit" – means an academic or administrative office, department, or division.

"Confidential Information" -- means information, whether transmitted orally or in writing, which is obtained by reason of the public position or office held and is of such nature that it is not, at the time of transmission, a matter of public record or public knowledge.6

1 S.C. Code. Ann. § 30-2-10 et seq.

2 S.C. Code Ann. § 30-2-20 (Privacy policies and procedures required of all state entities)

3 S.C. Code Ann. § 30-2-40 (Display of privacy policy on web site; access to personal information disclosure; criminal justice and judicial agency exception)

4 For purposes of this Policy and Procedure, the term Freedom of Information Act means the South Carolina Freedom of Information Act, codified at S.C. Code Ann. § 30-4 10 et seq.

5 The definitions derived from relevant provisions of laws, rules and regulations are cited after each.

6 S.C. Code Ann. §8-13-100(7)

"Education Records" – means those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

The term "education records" does not include (i) records of instructional, supervisory, and

administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute; (ii) records maintained by the Depart of Public Safety of the College that was created by that law enforcement Unit for the purpose of law enforcement; (iii) in the case of persons who are employed by the College but who are not in attendance as a student at the College, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or (iv) records on a student which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.7

“Employee Records” -- shall include the following: (a) the employment application (including background checks); (b) all human resources actions reflecting the employee's work history with the College; (c) documentation directly related to the employee's work record; and (d) all performance evaluations.8

“Identifying Information” -- includes, but is not limited to: (a) Social Security Numbers;
(b) driver's license numbers; (c) checking account numbers; (d) savings account numbers; (e) credit card numbers; (f) debit card numbers; (g) personal identification numbers; (h) electronic identification numbers; (i) digital signatures; (j) other numbers or information which may be used to access a person's financial resources; or (k) identifying documentation that defines a person other than the person presenting the document. This includes, but is not limited to, passports, driver's licenses, birth certificates, immigration documents, and state-issued identification cards.9

“Medical Record” or “Health Information” means any information, whether oral or recorded in any form or medium, that:

(1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) relates to the past, present, or future physical or mental health or condition of an

7 20 U.S.C. §1232g(a)(4)

8 S.C. Code Regs.19-720.02

9 S.C. Code Ann. §16-13-510(C)

individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.10

“Proprietary Data of the College” -- means all operational, scientific, business, personnel, student, donor, and all other information and financial knowledge and data owned, licensed, possessed, or controlled by the College including, but not limited to, the College’s methods of conducting its business affairs, methods, processes, systems, improvements, development and other plans, fund raising methods, trade secrets, and all other private matters. Trade secrets include feasibility, planning, and marketing studies, and evaluations and other materials which contain references to potential customers, competitive information, or evaluation.

"Personal Information" -- means information that identifies or describes an individual including, but not limited to, an individual's photograph or digitized image, Social Security Number, date of birth, driver's identification number, name, home address, home telephone number, medical or disability information, education level, financial status, bank account numbers, account or identification number issued by or used, or both, by any federal or state governmental agency or private financial institution, employment history, height, weight, race, other physical details, signature, biometric identifiers, and any credit records or reports.11

“Protected Information” -- is a single term that includes all of the following: Confidential Information, Educational Records, Employee Records, Identifying Information, Medical Record or Health Information, Personal Information, and Proprietary Data of the College.

"Public Record" -- includes all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body. Records such as income tax returns, medical records, hospital medical staff reports, scholastic records, adoption records, records related to registration, and circulation of library materials which contain names or other personally identifying details regarding the users of public, private, school, college, technical college, university, and state institutional libraries and library systems, supported in whole or in part by public funds or expending public funds, or records which reveal the identity of the library patron checking out or requesting an item from the library or using other library services, except non identifying administrative and statistical reports of registration and circulation, and other records which by law are required to be closed to the public are not considered to be made open to the public under this Interim Policy and Procedure.

Public Records include the following: (1) the names, sex, race, title, and dates of employment of all employees and officers of the College; (2) administrative staff manuals and instructions to staff that affect a member of the public; (3) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases; (4) those statements of policy and interpretations of policy, statute, and the Constitution which have been adopted by the College;
(5) written planning policies and goals and final planning decisions; (6) information in

or taken from any account, voucher, or contract dealing with the receipt or expenditure of public or other funds by the College; (7) the minutes of all proceedings of the Trustees and all votes at such proceedings, with the exception of all such minutes and votes taken at meetings closed to the public pursuant to S.C. Ann Code Section 30-4-70; (8) reports which disclose the nature, substance, and location of any crime or alleged crime reported as having been committed. Where

10 Title 45 Code of Federal Regulations § 160.103
11 S.C. Code Ann. §30-2-30(1)

a report contains information exempt as otherwise provided by law, the College may delete that information from the report.12

"Security Breach" – means the unauthorized disclosure of Protected Information. The Privacy Committee (see Section 15.0) will classify such Breaches by various levels of severity that will, in turn, specify the types of College responses appropriate to the level of severity the breach is assigned.

2.0 GENERAL RULES
2.1 Non-Disclosure. Protected Information may NOT be released to or shared with:

(a) any member of the public unless there is applicable statutory exception or an exception under College policy that authorizes the release of such Information; or

(b) any member of the College community unless the recipient has a legitimate interest for the use of that Protected Information to perform a service or carryout a responsibility within that person's scope of employment or engagement as a public official.

2.2 Procedure. Protected Information may only be released or shared in accordance with this Policy and Procedure.

2.3 Legal Determinations. Determinations of whether a particular element of Protected Information should be shared or released because it meets a statutory exception shall be made by the College Office of Legal Affairs, in consultation with the appropriate Executive Vice President and/or person responsible for the maintenance or distribution of the Protected Information, as circumstances may indicate.

2.4 Coverage. A person having access to Protected Information is expected to protect that Information from unauthorized disclosure. This includes, as appropriate:

Computer System and Applications Security: Central processing units, peripherals, portable storage devices, operating system, applications software and data.
Physical Security: The premises occupied by the College personnel or College contractors using computer equipment storing or having access to Protected Information.
Operational Security: Environment control, power equipment, operational activities related to operations.

Procedural Security: Established and documented security processes for information technology staff, vendors, management, and individual users of Protected Information.

12 S.C. Code Ann. §§30-4-20(c) and 30-4-50

Network Security: Communications equipment, transmission paths, switches, terminals and adjacent areas.

3.0 SPECIAL RULES DEALING WITH SOCIAL SECURITY NUMBERS13

3.1 Except as provided in Section 3.2 below, no Unit of the College shall –

(a) collect a Social Security Number or any portion of it containing six digits or more from an individual unless authorized by law to do so, or unless the collection of the Social Security Number is otherwise imperative for the performance of that Unit's duties and responsibilities, as prescribed by law or formal College policy. Social Security Numbers collected by a College Unit must be relevant to the purpose for which collected and must not be collected until and unless the need for Social Security Numbers has been clearly documented and approved (See Section 3.1.1);
(b) fail, when collecting a Social Security Number or portion of it containing six digits or more from an individual, to segregate that number on a separate page from the rest of the record, or as otherwise appropriate, so that the Social Security Number may be easily redacted pursuant to a public records request;
(c) fail, when collecting a Social Security Number or any portion of it containing six digits or more from an individual, to provide, at the time of or before the actual collection of the Social Security Number by that College Unit, upon request of the individual, a statement of the purpose or purposes for which the Social Security Number is being collected and the intended uses of the Number (see Appendix B and Section 3.5(a));
(d) use the Social Security Number or a portion of it containing six digits or more for any purpose other than the purpose stated for its collection;
(e) intentionally communicate or otherwise make available to the general public an individual's Social Security Number or a portion of it containing six digits or more or other Personal Identifying Information, except as otherwise allowed by law or these Policies and Procedures;
(f) intentionally print or imbed an individual's Social Security Number or a portion of it containing six digits or more on any card required for the individual to access College services;
(g) require an individual to transmit the individual's Social Security Number or a portion of it containing six digits or more over the Internet, unless the connection is secure or the social security number is encrypted;
(h) require an individual to use the individual's Social Security Number or a portion of it containing six digits or more to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site;

(i) print an individual's Social Security Number or a portion of it containing six digits or more on materials that are mailed to the individual, unless state or federal law requires the social security number be on the mailed document; or

13 S.C. Code Ann. §30-2-310 and §30-2-320

(j) require an individual to disclose her/his Social Security Number as a condition for receiving any College service or benefit unless such disclosure is required by law or this Policy.

3.1.1 Procedure. Attached to this Policy and Procedure and marked as Appendix C is a specific listing of the approved Uses of Social Security Numbers. Appendix D is a Social Security Number User Justification Form that must be completed and approved by the Policy Committee prior to the collection and use of Social Security Numbers. Unless otherwise requested by the College Privacy Committee and approved by the General Counsel in the office of Legal Affairs, the provisions of the previous sentence dealing with the use of Social Security Number User Justification Form shall not apply to data collection activities commenced prior to August 1, 2009.

3.2 Exemption. A College Unit that collects and uses Social Security Numbers or other Personal Identifying Information as part of the maintenance and reporting of employment records or the administration or provision of employee benefits programs is exempt from the prohibitions in section 3.1. Such a College Unit, however, shall adopt its own internal operating procedures that implement these prohibitions to the maximum extent practicable consistent with its mission and responsibilities.

3.3 Release of Social Security Numbers. Social Security Numbers and identifying information may be disclosed by the College:

(a) to another governmental entity or its agents, employees, or contractors, if disclosure is necessary for the receiving entity to perform its duties and responsibilities, including a debt collected pursuant to the Setoff Debt Collection Act, S.C. Code Ann. Section 12-56-10, and the Governmental Enterprise Accounts Receivable Collections program, S.C. Code Ann. Section 12-4-580. The receiving governmental entity and its agents, employees, and contractors shall maintain the confidential and exempt status of those numbers;

(b) pursuant to a court order, warrant, or subpoena;

(c) for public health purposes;

(d) on a document filed in the official records of the county;

(e) for employment verification or in the course of administration or provision of employee benefit programs, claims, and procedures related to employment including, but not limited to, termination from employment, retirement from employment, injuries suffered during the course of employment, and other such claims, benefits, and procedures;14 and

(f) as otherwise specifically allowed by law.

3.4 Physical Security of Social Security Numbers. College personnel shall not --

14 Subsections (a) through (e) found in S.C. Code Ann. § 30-2-320.

(a) collect, store or transmit Social Security Numbers as data elements to external entities until a business requirements submitted and approved in accordance with Section 3.1.1 (see also Appendix D);
(b) provide access to servers housing databases to College records containing Social Security Numbers data or other Personal Information unless the host has a firewall and other technical security measures as deemed appropriate by the Office of Information Technology; or
(c) except as provided in Section 10.0 of this Policy and Procedure, store Social Security Number data or other Confidential Information on removable or transportable media (such as paper forms, reports, cassettes, CDs, and USB/flash drives, laptops, mobile storage devices) or personal computers (such as PDAs and home computers).

3.5 Notice and Retention.

(a) When the collection of Social Security Numbers is required by law or permitted by College Policy, the College Operating Unit collecting the information shall provide the individual with a copy of, or electronic access/reference to this Policy and Procedure. Upon request, the Unit shall inform the individual whether the disclosure is mandatory or voluntary, the statutory or other authority under which the College is soliciting the number, and what uses will be made of the number. A subsequent request for production of a Social Security Number for verification purposes dealing with that same usage does not require the provision of another notice. Except for good cause that is documented in the appropriate file, the notice required under this subsection (a), if requested, shall be in writing (see Appendix B).

(b) Systems of records containing Social Security Numbers or other Personal Information shall be maintained for such periods of time as may be required under the College's Records Retention Policy (http://www.cofc.edu/~rr/), except that the General Counsel for the office of Legal Affairs may extend such time periods with respect to certain records as may be required to comply with court orders or rules, lawfully issued subpoenas or other compulsory process, or to otherwise mitigate legal risks to the College.

4.0 REQUESTS FOR EMPLOYEE RECORDS UNDER THE FREEDOM OF INFORMATION ACT15

4.1 Generally. In response to requests for information from Employee Records, the College may provide an employee's name, date of employment, title, sex, and race. The determination to disclose other types of information will be made on a case-by-case basis. To the extent practicable, the College shall inform the employee that a request has been

made regarding that employee.

15Implementation of this section will be in accord with the provisions of S.C. Code Ann. §41-1-65 and the
Freedom of Information Act S.C. Code Ann. §30-4-10 et seq.

4.2 Salary Information. Requests for salary information will be answered in accordance with the Freedom of Information Act.

4.3 Inquires by Prospective Employers.16 In responding to requests for information concerning current or former employees by prospective employers, the College may provide information as follows:

(a) when responding to oral requests for information, an employee's or former employee's dates of employment, pay level, and wage history;

(b) when responding to written requests, the following information, to which an employee or former employee may have access:

(1) Written employee evaluations;

(2) Official human resources notices that formally record the reasons for separation;

(3) Whether the employee was voluntarily or involuntarily released from service and the reason for the separation; and

(4) Information about job performance.

(c) No one shall knowingly or recklessly release or disclose false information.

4.4 Job Selection Information -- The College may, but is not required to, exempt from disclosure all materials, regardless of form, gathered by the College during a search to fill an employment position, except that materials relating to not fewer than the final three applicants under consideration for a position must be made available for public inspection and copying. In addition to making available for public inspection and copying the materials described in this Section 4.4, the College shall disclose, upon request, the number of applicants considered for a position. For the purpose of this section, materials relating to not fewer than the final three applicants, do not include an applicant's income tax returns, medical records, Social Security Number, or information otherwise exempt from disclosure by the Freedom of Information Act.17

5.0 EDUCATION RECORDS

Policies and procedures dealing with the disclosure of education records shall be in accord with the policies of the College Registrar dealing with the implementation of the

Federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g). Those policies and procedures can be found at: http://www.cofc.edu/~register/FERPA.htm. Interpretations of the statute and the controlling regulations shall be made by the Office of Legal Affairs, after consultation with the Office of the Registrar, or the Provost, as may be appropriate under the circumstances.

16 See S.C. Regs. Ann. 19-720.03(B)
17 S.C. Code Regs. §19-703.05

6.0 "MEDICAL RECORD" or "HEALTH INFORMATION"

6.1 Disclosure. Medical Records of employees and students may only be released or shared in accordance with the provisions of the South Carolina Physicians' Patient Records Act (S.C. Code Ann. § 44-115-10 et seq.), the Federal Family Educational Rights and Privacy Act, and such other provisions of state or federal law as may be applicable.
6.2 Interpretations. The South Carolina Physicians' Patient Records Act (S.C. Code Ann. § 44-115-10 et seq.) states in part:
Except as otherwise provided by law, a physician shall not honor a request for the release of copies of medical records without the receipt of express written consent of the patient or person authorized by law to act on behalf of the patient. (§ 44-115-40) (emphasis supplied)
For the purposes of this Policy and Procedure, the College will afford any licensed health care provider within the employ of the College the same protection afforded a "physician" under the above cited statute. The term "Except as otherwise provided by law" shall be subject to interpretation by the General Counsel for the office of Legal Affairs.
6.3 Health Insurance Portability and Accountability Act of 1996 ("HIPAA") . While neither the College nor any Unit of the College is currently subject to HIPAA, the College may elect, in the exercise of its discretion, to utilize such forms dealing with the disclosure or release of Medical Records as may be compliant with HIPAA.

7.0 DISPOSAL OF INFORMATION TECHNOLOGY RESOURCES CONTAINING PROTECTED INFORMATION18
7.1 Hardware and Storage Media. Before a College Unit may transfer or dispose of information technology hardware or storage media, all Protected Information must be removed and the hardware and storage media must be sanitized in accordance with the standards and policies adopted by the Chief Information Officer ("CIO"). The CIO shall verify that all Protected Information is removed and the information technology hardware and storage media are sanitized in accordance with those standards and policies before the transfer or disposal occurs.

7.2 Records. When a College Unit disposes of a record that contains Protected Information the Unit shall modify, by shredding, erasing, or other means, the Protected Information to make it unreadable or undecipherable. The College Unit is considered to comply with this requirement if it uses a College retained contractor who is engaged by the College and who is in the business of disposing of such records.

8.0 ETHICS

8.1 Self-Dealing. An employee of the College may not use or disclose Protected Information gained in the course of or by reason of that person's official responsibilities in a way that would affect an economic interest held by that person, a member of that person's immediate family, or an individual or business with whom that person is associated.

8.2 Misuse of Records. An employee of the College may not willfully examine, or aid and abet in the willful examination of a workers' compensation record, a record in connection with health or medical treatment, social services records, Employee Record, Education Record, or other records of an individual in the possession of or within the access of the College if the purpose of the examination is improper or unlawful.

9.0 RESPONSIBILITIES

9.1 Passwords. Passwords help protect against misuse of data systems and networks by restricting the use of those systems and networks to authorized users. Each authorized user of such a system may be assigned or may be asked to develop a unique password that is to be protected by that individual and not shared with others, is difficult to determine, is changed on a regular basis, and is deleted when no longer authorized.

9.2 Security. Individual users are responsible for ensuring that others do not use their system privileges. In particular, users must take great care in protecting their usernames and passwords from eavesdropping, loss or careless misplacement. Passwords are never to be 'loaned.' Individual users will be held responsible for any security violations associated with their username or passwords.

9.3 Access Policies of Data Systems. Each user permitted to access a system containing Protected Information shall be made aware of the access policy for that system. Management will provide this information to the employee when first granting access and make the employee aware of the auditing capability in place to verify compliance.

9.4 Collection of Protected Information. As Protected Information is developed or compiled, the individual(s) responsible for the development or collection of the data are responsible for assuring that storage and access of the data is appropriately managed.

9.5 Audit of Systems Containing Protected Information. Information Technology operations staff are responsible for reviewing the logs and identifying potential security violations. The IT operations staff is responsible for establishing the security and access control mechanisms (such as usernames, passwords, and logging protocols) and may be held accountable for any security breaches that arise from improper configuration of these mechanisms. If the application is housed outside of IT, the application administrator must be in a position to fulfill these requirements and document the same in writing.

10.0 PROTECTED INFORMATION STORED ON COMPUTING DEVICES19

10.1 Generally. Protected Information that resides on a College user's computer or a portable computer or portable storage device must be secure at all times. The theft or loss of a portable computer or portable storage device must not put Protected Information at risk of unauthorized disclosure. In addition, Protected Information shall not be maintained at all, if to do so would violate the College's records retention policy dealing with the length of time such records should be maintained (see http://www.cofc.edu/~rr/).

10.2 Consultation with IT. Members of the College community who have a legitimate business or educational need to take Protected Information off campus in the form of a portable electronic device shall consult with the College Chief Information Officer or his/her designee for the nature and type of protection that shall be afforded such Information.

11.0 USE OF INFORMATION TECHNOLOGY SYSTEMS FOR ILLEGAL PURPOSES

The College does not randomly monitor the content of personal e-mails, downloads, or other on- line communications or data transmissions that pass through, are resident on, or that otherwise use the College's IT resources. The College, however, reserves the right to examine its computer records, or to monitor activities of individual computer users of the College IT system, if it has a reasonable belief that such action is needed to: (a) protect the integrity or security of the computing resources; (b) protect the College from incurring liability; (c) investigate unusual or excessive activity typically associated with illegal or illicit activity; (c) investigate reasonably suspected violations of law or College policy; or (d) comply with law or compulsory legal process (such as a lawfully issued subpoena). All such actions must be reviewed and pre- approved by the General counsel for the office of Legal Affairs who shall consult with the President or the appropriate Executive Vice President, as the circumstances may warrant.

12.0 INTERNET AND EMAIL ACCESS

12.1 Vulnerability of Systems; Transmissions. Protected Information shall not be saved on any computer directly accessible from the Internet or from "open" portions of College's internal network unless a user must first be duly authorized to access such open portions. Users should clearly understand that many common systems, such as normal email, cannot be considered a secure way to transport confidential information. If it is necessary to transmit Protected Information electronically to a point external to the College, prior consultation should take place with the Office of the CIO.

12.2 Web Based Surveys and Other Data Collection Tools. Data collection tools, such as web based surveys that request Confidential Information, must ensure that responses cannot be accessed by unauthorized persons and that Personal Information is not improperly disclosed or shared. If a College vendor is involved in conducting the survey or analyzing results that include Confidential Information that can be linked to individuals, a contract must be in place that protects the Protected Information.

13.0 SECURITY BREACHES

Every member of the College community who reasonably believes that a Security Breach has occurred is under an affirmative obligation to report that Breach as soon as practicable to the Office of the CIO and the Office of Legal Affairs. The Security Breach shall be assigned a preliminary level of severity appropriate to the potential of the Breach to result in identity theft, invasions of privacy, and/or economic or other harm to the College. The CIO shall consult with the General Counsel for the office of Legal Affairs and privacy Committee regarding all such matters.

14.0 COMPLIANCE

14.1 Consequences for Violations. All individuals accessing Protected Information are required to comply with federal and state laws and College policies and procedures regarding such Information. Any College employee or student who engages in the unauthorized use, disclosure, alteration, or destruction of data in violation of this Policy and Procedure will be subject to appropriate disciplinary action, including possible dismissal and/or legal action. Other persons who may violate this Policy and Procedure, such as a College vendor, may be barred from College property and any further business dealings with the College, as well as, appropriate legal action. The College reserves the right to require anyone having access to Protected Information to first execute a confidentiality agreement http://newdev.eecs.harvard.edu/p- 02.10.htm approved by the Office of Legal Affairs as a condition for having access to such Information.

14.2 Responsible Office. The Office of the CIO shall be responsible for monitoring compliance with this Policy and Procedure and for reporting violations to the appropriate Executive Vice President and to the Office of the Legal Affairs. The General Counsel for the office of Legal Affairs shall be responsible for determining if there is reason to believe that any law, rule, or regulation may have been violated.

15.0 COMMITTEES

15.1 Privacy Committee.

(a) Privacy Committee Establishment and Purpose. There is hereby established a College of Charleston Privacy Committee that shall act to: (1) review and keep current with federal, state and local laws and regulations concerning privacy and information stewardship; (2) review campus-wide information collection, storage, management, and dissemination methods and practices to ensure compliance with such laws and regulations; (3) recommend policy and procedures dealing with data stewardship and the responsibilities of data stewards; (4) make recommendations on proposals to collect and use Social Security Numbers (see Section 3.1.1 and Appendix D); (5) investigate and take appropriate actions with respect to security breaches and
(6) assess overall compliance with this Policy and Procedure, as it may from time to time be modified, and make such recommendations for further modifications as may be appropriate.

(b) Privacy Committee Membership and Meetings.

Unless otherwise indicated in this subsection (b), the Privacy Committee shall be comprised of the following or their designees: Executive Vice President for Business Affairs, the Provost, Executive Vice President Advancement/Development, the Speaker of the Faculty, the President of the Student Government Association and, on a non-delegable basis, the Senior Vice President for Technology/CIO, Dean of Students, Director for Human Resources, Associate Vice President of Institutional Research, and the Internal Auditor. Legal advice to the Committee shall be provided by the Office of Legal Affairs. The committee will meet, and report on its meeting to the Executive Team, at least 4 times per academic year and at such other times as may be required to fulfill its purpose. From time to time the President shall appoint a Chair of the Committee.

15.2 Information Security Committee.

(a) Information Security Committee Establishment and Purpose. There is hereby established a College of Charleston Information Security Committee that shall report to the Privacy Committee. The Information Security Committee shall act as both an oversight and an implementation Committee with respect to the assessment, investigation and implementation of the technical measures needed to provide for system security and the security of Protected Information. This Committee shall ensure that such technical measures are taken as may be necessary or appropriate to implement and maintain this Policy and Procedure. Among other things, the Committee shall: (1) develop procedures, guidelines, and best practices training and awareness related to the technology infrastructure of the College to ensure the responsible collection, storage, use and safekeeping of Protected Information by the College community in accordance with this Policy and Procedure; and (2) upon consultation with the Chair of the Privacy Committee and the General Counsel for the office of Legal Affairs, take such actions in response to Security Breaches, including audits and investigations, as may be appropriate under the circumstances.

(b) Information Security Committee Membership and Meetings. The Information Security Committee shall be chaired by the Senior Vice President for Technology/CIO and shall be comprised of representatives from the following: (1) Data Stewards; (2) Office of Institutional Research; (3) Marketing and Communications; (4) Director, Information Services; (5) Director, Programming and Network Services; (6) Director, Infrastructure Services; and (7) such other Information Technology staff as may be determined by the Senior Vice President for Technology/CIO. Legal advice to the Committee shall be provided by the Office of Legal Affairs. The Committee will meet at least 4 times per academic year and at such other times as may be required to fulfill its purpose. The Information Security Committee shall be responsive to the inquires and requests of the Privacy Committee and shall report on its activities to the Privacy Committee at least once a calendar quarter and at such other times as may be requested by the Chair of the Privacy Committee.

15.3 Limitation on Authority.

The information systems that may be reviewed by the Committees established under this Section
15.0 shall include, but not be limited to, those systems containing records on promotion and tenure, post tenure review, student judicial affairs, employee and student discipline, health and counseling services, research, advancement, employees, students, vendors, business transactions, and such other matters and records as the committees may deem appropriate, provided that nothing contained in this section shall be deemed to authorize any Committee member to have access to Protected Information that s/he would not otherwise have access to under other provisions of this Policy and Procedure.

16.0 DISTRIBUTION

All College managers having access to Protected Information, or having supervision or responsibility for individuals having access to Protected Information, are responsible for disseminating this Policy and Procedure to such persons. This Policy and Procedure shall be published on the College's web site.

17.0 AMENDMENTS

This Privacy Policy and Procedure may be amended at anytime in accordance with the Colleges
Campus Wide Policy Making Procedures.

****

APPENDIX A
NOTICE REQUIRED BY SOUTH CAROLINA ANN. CODE 30-2-40(B)20

Suggested Format of Notice:

Please be advised that part or all of the information you are being requested to provide the College is considered "Personal Information" because it can be used to identify you or describe you. Some of this information may be subject to public scrutiny and release under the South Carolina Freedom of Information Act (S.C. Code Ann. §30-4-10 et seq.). However, in the absence of a court order or other legal compulsory process the College will not publicly release information of a personal nature when the public disclosure would constitute an unreasonable invasion of your personal privacy or when the information requested is otherwise exempt from mandatory disclosure under the Freedom of Information Act (see
S.C. Code Ann. § 30-4-40).

Further questions regarding the College Privacy Policy may be directed to the College's General Counsel for the office of Legal Affairs.

****

20 The statute reads as follows:
§ 30-2-40. Display of privacy policy on web site; access to personal information disclosure; criminal justice and judicial agency exception.

(A) Any state agency, board, commission, institution, department, or other state entity which hosts, supports, or provides a link to page or site accessible through the world wide web must clearly display its privacy policy and the name and telephone number of the agency, board, commission, institution, department, or other state entity person responsible for administration of the policy.
(B) Where personal information is authorized to be collected by an entity covered by this section, the entity must at the time of collection advise the citizen to whom the information pertains that the information is subject to public scrutiny or release.
(C) Subsection (B) does not apply to criminal justice or judicial agencies, or both.

APPENDIX B
STATEMENT OF PURPOSE FOR THE COLLECTION OF SOCIAL SECURITY NUMBERS21
Suggested Format of Response Upon Request:

The College is collecting your Social Security Number for the following purpose or purposes22:

□ Enrollment:

□ Employment:

□ Employee Benefits:

□ Payment for Personal or Professional Services; Other Disbursements:

□ Insurance Providers:

□ Third Party Sponsors of Student Aid:

□ Credit Card Information:

□ Public Safety:

□ Otherwise Required By Law:

21 South Carolina law provides in relevant part:
§ 30-2-310. Collection of and maintenance and disposition of records containing social security numbers by public agencies.

(A)(1) Except as provided in Sections 30-2-320 and 30-2-330 of this article, a public body, as defined in Section 30- 1-10(B), may not:
(a)) …
(b)) …
(c) fail, when collecting a social security number or any portion of it containing six digits or more from an individual, to provide, at the time of or before the actual collection of the social security number by that public body, upon request of the individual, a statement of the purpose or purposes for which the social security number is being collected and used;

22 See Appendix C for a fuller statement of permissible purposes and summarize the applicable purpose in the space provided for in this form.

APPENDIX C

APPROVED USES OF SOCIAL SECURITY NUMBERS AND OTHER PERSONAL INFORMATION

The primary approved uses and the reasons for collecting and maintaining Social Security Numbers ("SSNs") and other Personal Information by of for the College of Charleston include, but are not limited to, the following:

Enrollment:

Those wishing to enroll in academic offerings at the College, both credit and non-credit, may be required to provide a SSN to determine lawful presence in the United States. With respect to student employment, IRS regulations require the College to request a SSN as a Taxpayer ID number for use in tax reporting. In addition, any student applying for financial aid may be required to provide a SSN to the College. Historic records may retain a student's SSN if, for example, the SSN was previously used as the primary identifier for the person who is the subject of that record. However, to the extent practicable, the release of such a record to other than the subject should be preceded by an inquiry with the subject if he/she would prefer if the College redact the SSN from the record.

Employment:

A SSN must be provided on Form I-9 (Employment Eligibility Verification) in accordance with the Immigration Reform and Control Act of 1986 (IRCA). SSN's may also be collected to verify lawful presence in the United States through E-Verify and other acceptable verification sources. Finalist for employment may also be requested to provide a SSN

pursuant to the College's Background Checks Policy. All persons employed by the College must also provide a SSN as the taxpayer ID number. Providing a valid SSN is a condition of employment.

Employee Benefits: If required by law or a benefits provider, the SSNs of the employee and the employee's dependents/beneficiaries may be collected and provided to the service provider.

Payment for Personal or Professional Services; Other Disbursements: Any person providing services to the College as a contractor, invited speaker or research subject for which payment will be made, may be required to provide a SSN as the taxpayer ID number. These taxpayer ID numbers may be stored in the accounting system as part of the vendor record. In addition, certain other disbursements from the College may require reporting to the Internal Revenue Service. In such an event, these disbursements may be preceded by a request for the SSN or other taxpayer ID number.

Planned Giving Donors: Donors to the College participating in planned giving programs must provide a SSN as the taxpayer ID.

Insurance Providers: SSNs continue to be the patient identifier for many health care providers. To enable payment of medical bills, and to the extent allowed by law, the SSN of the patient may be shared with the insurance company providing health coverage.

Third-Party Sponsors of Student Aid: Various third-party sponsors of student aid, including several state agencies, require the submission of SSNs for those students for which aid is being provided. In order for the sponsor to make payment to the College, a SSN may be requested for proper verification.

Credit Card Information: When the College has been paid by credit or debit card, or a declining balance card, the College may maintain the card numbers and related information for a period of time, in accordance with its records retention policy, after the transaction has occurred.

Student Health Services: SSN's or other personal identifying information may be used, as appropriate, as a patient identifier for referrals and consultation with outside medical providers and for communication with insurance companies.

Public Safety: Law enforcement personnel may collect or use SSN data to serve a subpoena, conduct an investigation, to make a report, or to make an arrest, as permitted by applicable provisions of state and federal law, rules or regulations. Additionally, Campus Police maintain copies of fingerprint cards for Public Safety employees and others that may contain SSN data and other Personal Information.

Otherwise Required By Law: As determined by the General Counsel for the office of Legal Affairs, Personal Information shall be collected, used and maintained as directed by court order, subpoena or other compulsory legal process, or as otherwise required to protect the legal interests of the College and the College community.

APPENDIX D

SSN USAGE JUSTIFICATION FORM[23]

Requestor Name _____ Date _____
Department _____ Phone _____
Address _____ E-Mail _____

Briefly describe why and under what authority you believe SSN's must be collected.			
Briefly describe the process you intend to use for the collection of the SSN and the notice you intend to provide to the providers of their SSN's.			
Describe how the SSN will be stored including the types of media used for both primary and backup storage and what security measures will be employed.			
Will the data be stored on any portable equipment or media? If so, please describe how this will be used and what type of security measures will be used.			
Will the SSN be used as a primary identifier?			
List the approximate number of individuals Requiring access to the SSN data you retain.	Faculty	Staff	Students
Describe the method(s) used to access the SSN and what controls will be implemented to manage the access. Who will be the Steward for this information?			

_____ _____
Department Head/Manager Signature Date

_____ _____
Dean (If Applicable) Signature Date

Recommendation of the Privacy Committee:

_____ _____
_____ Date

Approval:

_____ _____
Executive Vice President Signature Date

[23] To be filed with and maintained by the Division/Department Head.

Departments/Offices Affected by the Policy

All Departments

Procedures Related to the Policy

Related Policies, Documents or Forms

Issue Date: 8/23/2016 **Date of Policy Revision:8/23/2016**	**Next Review Date:10/23/2020**

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

Policy Number: 11.1

President or
Chairman, Board of Trustees [signature] Date: 8/23/16