Policy: Confidentiality Policy	**Policy No:** I-6.4
Policy Owner(s): Human Resources	**Original Date:** 3/10/2006
Last Revised Date: 4/27/2022	**Approved Date:** 6/1/2022

I. **POLICY**: Under Ohio Revised Code § 1333.81, an employee is legally obligated to not disclose an employer's confidential, non-public or proprietary information received during employment to any third party without consent of the employer. Consistent with this law, John Carroll University ("the University" or "JCU") requires that its employees not disclose, publicize or discuss any Confidential Information (hereinafter "Confidential Information") belonging to or related to the University to any Constituent within the University who does not have a legitimate need-to-know, or to any third party outside the University when not required to carry out University duties, required by law, or without the written consent of the University.

In addition, John Carroll University employees are required to maintain confidentiality of a student's educational records unless the disclosure is permitted by the Family Educational Rights and Privacy Act (FERPA). Furthermore, certain employees who have access to health care records protected under the Health Insurance Portability and Accountability Act (HIPAA), such as medical plan information, are obligated to maintain confidentiality of those records under federal law.

II. **PURPOSE**: John Carroll University utilizes and maintains various non-public, proprietary and confidential databases, electronic information, paper records, and other data and documents regarding University operations and Constituents. The Confidential Information contained in these records is intended exclusively for purposes related to the University's operations and planning. All John Carroll University employees have an obligation to respect the privacy of information regarding University Constituents, and to protect and maintain the confidentiality of all University non-public or proprietary information belonging to or regarding the University.

This policy is intended to set out the expectations JCU places on employees to adhere to laws and policy on maintaining and safeguarding confidential, non-public or proprietary information of the University. This Confidentiality Policy reflects the governing federal and Ohio laws that legally require employees to keep certain information confidential, during and after the term of employment at JCU.

III. **SCOPE**: All employees, volunteers, board members, student employees, and contractors of John Carroll University

IV. **DEFINITIONS:**

Confidential Information: oral, written, electronic and other private, non-public or proprietary information accessible to an employee through the course of the employee's employment with the University or provided by JCU to an employee that relates in any way to JCU, its employees, students or business operations.

Confidential Information shall not include any information which:

i. is at the time of disclosure available to the public (other than as a result of a disclosure directly or indirectly by the employee);

ii. is, prior to the start of the employment with JCU, already in the possession of or known to the employee; and/or

iii. was obtained by the employee, either prior or subsequent to disclosure by JCU, from a third party not under any obligation of confidentiality to JCU.

Confidential information includes, but is not limited to:

- Any internal and non-public University financial statements and statistical and narrative reports;
- Employee and applicant records and files, and statistical reports containing the same;
- Student and applicant records and files, demographic data, and statistical reports containing the same;
- Computer authorization/security codes/passwords;
- Any non-public administrative minutes and records of internal University committees;
- Non-public or proprietary academic or accreditation materials and records;
- Non-public Board of Directors and other administrative materials and minutes;
- Information related to donors or prospective donors, and other non-public development records and materials; and/or
- Non-public or proprietary information regarding University strategic and operational plans, processes, or documents.

Constituent: Constituents include all faculty, staff, students, volunteers, University Board of Directors members, University donors, prospective donors and alumni.

V. PROCEDURES:

a. Employees shall not disclose, publicize or discuss to or with any third party any non-public, proprietary and Confidential Information related to the University ("Confidential Information") that they have access to or are provided in the scope of their work with the University, unless the University provides written consent or the third party or internal Constituent who has a legitimate need-to-know. Employees must maintain strict confidentiality of all Confidential Information at all times, both at work and outside the work setting. Employees also are required to maintain confidentiality of all student educational records protected under FERPA and all protected health information protected by HIPAA, consistent with those applicable federal laws and regulations.

b. Access to University electronic records and databases is authorized and granted pursuant to the University Information Technology Resources and Sensitive Data and Security Policies and other related policies and procedures. Employees shall maintain confidentiality of all electronic Confidential Information or Sensitive Data, as defined by and consistent with those policies.

c. Employees should not discuss Confidential Information in open and/or public areas, including but not limited to hallways, open areas, stairwells, restrooms, and other public locations.

d. Confidential Information, in any format, may not be disclosed or distributed outside the University without approval of the appropriate divisional vice president, the chief information officer, and/or Human Resources, or their designees.

e. Confidential Information provided to University agents or contractors (i.e. consultants, data vendors, etc.) as part of University-related business or projects shall be disclosed only with appropriate written assurances from the agent or contractor of the obligation to maintain confidentiality as to the information. All third-party recipients and users of University Confidential Information are bound by this policy concerning confidentiality and must either 1) incorporate University-approved confidentiality clauses into their contracts and/or service agreements or 2) read and sign a University confidentiality agreement. Confidential Information distributed by the University to outside parties should contain a statement regarding the confidential nature of the information such as: "This Confidential Information has been compiled by John Carroll University for its exclusive use. It is not provided for private use of any third party, such as commercial solicitations or the expression of personal, political, social or other views. The information may not be reproduced, distributed, sold, or stored, either electronically

or otherwise, without the written consent of an authorized representative of JCU."

f. Confidential Information may not be disclosed to unaffiliated organizations or individuals for uses construed as third-party fundraising, solicitation, or marketing, unless an exception is made with the written approval of the appropriate divisional vice president. The use of such information for these purposes is limited to the University in service of advancing JCU's institutional mission and goals.

g. Although this obligation to maintain confidentiality operates by law without any written agreement of the employee, the employee may be asked by individual departments or related to individual duties or assigned projects to sign a confidentiality agreement setting out the obligations for maintaining confidentiality as to that department, duties or project.

h. It is the responsibility of any University employee or representative coordinating the distribution of Confidential Information to ensure that all distributed documents or data remain secure and are either returned or destroyed (i.e., shredded or electronically wiped) as needed and in accordance with appropriate records retention schedules.

i. All departments or individuals maintaining or storing Confidential Information must reasonably secure such information during business and non-business hours.

j. An unauthorized disclosure is also a breach of the University Code of Ethics.

k. If an employee does not know whether the information is non-public, proprietary, or confidential, then they should maintain confidentiality as to the information until they obtain clarification from their supervisor or division head as to the status of the information. Supervisors or division heads may confer with Human Resources or the Office of Legal Affairs regarding issues about Confidential Information.

l. All employees have the responsibility to report suspected violations of this Confidentiality Policy, as well as any suspected violation of applicable law or regulation.

    i. Employees are encouraged to report suspected violations to their supervisor or department head, to Human Resources, or to appropriate University officials designated in the applicable University policy.

    ii. No person who makes a good faith report of a suspected violation will be reprimanded or retaliated against in any way.

m. Any violation of this Policy or related laws or regulations will be investigated and may result in corrective action up to and including termination, or other appropriate actions, consistent with University policies.

n. An employee is barred from disclosing or utilizing Confidential Information after their employment at JCU is concluded. If an employee discloses Confidential Information to a third party without University consent, the University may pursue appropriate actions or legal recourse against the former employee.

VI. CROSS REFERENCE:

I-6.16 Code of Ethics Policy

I-3.2 Health Insurance Portability and Accountability Act
Office of Registrar, FERPA- https://jcu.edu/registrar/students/ferpa

I-7.1 Information Technology Resources

Sensitive Data and Security Policy

Consent to Release Education Records - https://jcu.edu/sites/default/files/2019-06/REQUEST-TO-RELEASE-RECORDS-10-13-15.pdf

VII. ATTACHMENTS: