Overview

**Description:** In advancement of the Chief Information Officer’s operational responsibilities and in accordance with federal, state, local and international laws relevant to information privacy and security, this administrative regulation establishes Maricopa County Community College District ("MCCCD")'s commitment to protecting the integrity and privacy of Sensitive Information¹ and promoting meaningful online experiences² through implementation of business practices and technological measures for:

- Protecting Sensitive Information
- Collecting Sensitive Information
- Obtaining Sensitive Information
- Using Sensitive Information
- Accessing Sensitive Information
- Disclosing Sensitive Information
- Opting Out
- Correcting Sensitive Information

**Applicability:** Information Security is everyone’s responsibility. All MCCCD Personnel and Persons of Interest ("POIs"), whether through use of online technology resources³ or other formats, are covered by this administrative regulation. MCCCD students are expected to know and comply with all current published policies, rules and regulations as stated in the college catalog, class schedule, and/or student handbook.⁴

### Protecting Sensitive Information

MCCCD takes important steps to protect Sensitive Information. MCCCD treats Sensitive Information as confidential and encourages its Personnel and POIs to take care in handling it. MCCCD limits access to Sensitive Information to those who need it to perform their jobs. MCCCD’s external service providers must also protect Sensitive Information, and use it only to meet MCCCD’s business needs. MCCCD also takes steps to protect its computer systems from unauthorized access.

---

¹ Sensitive Information is information that is so deemed under applicable law. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Sensitive Information covered under the Arizona Revised Statutes (ARS), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.

² This administrative regulation addresses the District’s commitment to ensure productive experiences within the family of MCCCD Web sites. MCCCD is not responsible for the privacy statements or other content on Web sites outside of the MCCCD family of Web sites. MCCCD encourages individuals to review the privacy statements of Web sites they choose to link to from MCCCD to understand how those Web sites collect, use and share information.

³ MCCCD Administrative Regulation 4.4 Technology Resource Standards provides the following examples of technology resources: Websites, applications (such as, but not limited to, MCCCD’s Instructure/Canvas-based Course Management System and RioLearn Learning Management System), desktop and laptop systems, printers, central computing facilities, MCCCD-wide or college-wide networks, local-area networks, telephones, facsimile machines, scanners, access to the Internet, electronic mail and similar electronic devices and information.

⁴ See, for example, MCCCD Administrative Regulations 2.1 General Regulation, 2.5.1 Disciplinary Standards, and 2.5.2 Student Conduct Code.
MCCCD works diligently to comply with applicable information security, data privacy and related laws, rules and regulations. Student records are protected by the Family Educational Rights and Privacy Act (FERPA), Arizona law and MCCCD administrative regulations. Employee records are protected by MCCCD administrative regulations and by Arizona law.

As further protection of Sensitive Information and the privacy rights of individuals, MCCCD holds an Office for Human Research Protections (“OHRP”)-approved Federal-wide Assurance (“FWA”) and adheres to the U.S. Department of Health & Human Services (“HHS”) guidelines whenever MCCCD is engaged6 in human subjects research (“HSR”). The MCCCD Institutional Review Board (“IRB”) must review and approve all proposed HSR before it has begun.

Individually identifiable health information is protected from unauthorized release if there is a reasonable basis to believe the information can be used to identify the individual. MCCCD is required by the HIPAA Privacy Rule (the “Privacy Rule”) issued under HIPAA to maintain the privacy of protected health information. MCCCD is committed to fully complying with the Children’s Online Privacy Protection Act of 1998 to the extent that it is applicable. The Federal Trade Commission provides more information about the Children’s Online Privacy Protection Act.

**Collecting Sensitive Information**

In connection with hiring and admissions practices, MCCCD collects identifiable information, such as an individual’s name, e-mail address, home or work address, and telephone number. MCCCD also collects demographic information such as gender, age, zip code, and interests.

Pursuant to the HIPAA Privacy Rule and, for example, in connection with administration of its group health plans, provision of public safety practices, and operation of its medical and dental facilities, MCCCD adheres to standards of confidentiality regarding individually identifiable health information created or received by MCCCD that relates to the following:

1. Past, present, or future physical or mental health or condition;
2. Previously rendered health care services;
3. Planned health care services; and
4. Past, present or future payments for health care services.

MCCCD reserves the right to log and monitor all activity and all data on its systems and network(s). This may involve capturing and retaining a complete keystroke and click log of an entire session. In addition, MCCCD may search files on individual and networked technology resources7 to investigate a potential privacy violation.

5 [http://www.hhs.gov/ohrp/policy/engage08.html](http://www.hhs.gov/ohrp/policy/engage08.html)
6 See, MCCCD Administrative Regulation 3.8 MCCCD Institutional Review Board.
7 MCCCD Administrative Regulation 4.4 Technology Resource Standards provides the following examples of technology resources: Websites, applications (such as, but not limited to, MCCCD’s Instructure/Canvas-based Course Management System and RioLearn Learning Management System), desktop and laptop systems, printers, central computing facilities, MCCCD-wide or college-wide networks, local-area networks, telephones, facsimile machines, scanners, access to the Internet, electronic mail and similar electronic devices and information.
Information about computer hardware and software is collected by MCCCD. Web analytical tools that do not create individual profiles are used by MCCCD to analyze traffic to MCCCD websites. MCCCD uses these tools to routinely record the following information each time MCCCD's websites are used:

1. Internet address of the computer being used;
2. Web pages requested;
3. Referring web page;
4. Browser used;
5. Date, time and duration of activity; and
6. Volume of data storage and transfers.

MCCCD uses this information about website usage to monitor and preserve MCCCD website functionality and integrity. Analysis of this information also helps MCCCD improve access to web content based on browser types and operating system types, by enabling MCCCD to make web content available to as many online users as practical. MCCCD does not link this collected information to the personal information that an individual may actively submit online when participating in or registering for programs and activities.

Some MCCCD web pages use cookies to store information, and some web-based services require cookies for access. Cookies are short pieces of information used by web browsers to remember an individual's specific information on subsequent visits and to personalize the online experience. For example, if an individual personalizes MCCCD pages, or registers with MCCCD sites or services, a cookie may help MCCCD to recall their personal information, such as name, home address, phone number and other details. Cookies can be disabled on most personal computers by modifying the browser setting to decline cookies. If, however, cookies are declined, an individual may not be afforded a fully interactive online experience.

MCCCD accepts credit card payments online for a variety of goods and services. To prevent unauthorized access as the credit card information travels over the Internet, credit card information handled by MCCCD, such as the cardholder’s name, address and credit card number, is encrypted before transfer to any financial institution for further processing. Credit card transactions performed by students in self-service are encrypted when noted by the “lock” icon on the web page.
Obtaining Sensitive Information

In most cases, MCCCD obtains information about an individual from the individual. MCCCD may also use outside sources to help ensure its records are correct and complete. These sources may include background check companies, employers, other educational institutions, adult relatives, and others. These sources may give MCCCD reports or share what they know with others. MCCCD does not control the accuracy of information external sources provide to MCCCD. If an individual wants to make any changes to information MCCCD receives from others about them, they must contact those sources.

Using Sensitive Information

MCCCD collects information to help it decide whether an individual is eligible for enrollment into specific MCCCD courses, participation in specific MCCCD programs, and/or employment by MCCCD departments and offices. MCCCD may also need personally identifiable information to help deter fraud, money laundering, or other crimes. How MCCCD uses this information depends on what educational products and services an individual has or wants from MCCCD. It also depends on what laws apply to those educational products and services. For example, MCCCD may also utilize personally identifiable information and individually identifiable health information to:

- Verify financial aid eligibility and process related transactions
- Perform research on issues affecting community colleges and collaborate with other educational institutions and states to improve student success and institutional performance
- Confirm or correct an individual’s information
- Market new educational courses
- Help run and operate MCCCD
- Deliver requested educational services
- Establish eligibility for family medical leave, disability accommodation, and course and program placement
- Survey opinions of current services or potential new services
- Comply with applicable laws

Accessing Sensitive Information

Students: Information about the rights of a student to access their education records in compliance with FERPA is available at https://chancellor.maricopa.edu/public-stewardship/governance/administrative-regulations/2-students/2.5-student-rights-and-responsibilities/2.5.3-student-records.

Service Providers: From time to time, individuals or companies under contract with MCCCD may have authorized access to Sensitive Information in the course of the services they provide to MCCCD.

Disclosing Sensitive Information

MCCCD will not disclose Sensitive Information without notice, unless it is required to do so by law or it believes, in good faith, that such action is necessary to: (a) conform to law or comply with legal process, (b) safeguard and defend the rights or property of MCCCD, or (c) act under exigent circumstances to protect the life and/or personal safety of others. Confidential information protected by FERPA or by other laws or Board administrative regulations will not voluntarily be disclosed in response to a public records request.

Student information: Pursuant to FERPA, MCCCD must, except under certain conditions, obtain written consent for or on behalf of a student prior to the disclosure of certain information from the student’s education records. MCCCD may, however, disclose the following basic “directory information” that generally is not considered harmful or an invasion of privacy without consent:
<table>
<thead>
<tr>
<th>4.22 Statement on Privacy (cont'd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name</td>
</tr>
<tr>
<td>• Address</td>
</tr>
<tr>
<td>• Telephone number</td>
</tr>
<tr>
<td>• Major field of study</td>
</tr>
<tr>
<td>• Participation in officially recognized activities and sports</td>
</tr>
<tr>
<td>• Weight and height of members of athletic teams</td>
</tr>
<tr>
<td>• Degrees and awards received</td>
</tr>
<tr>
<td>• Dates of attendance</td>
</tr>
<tr>
<td>• Part-time or full-time status</td>
</tr>
<tr>
<td>• Most recent previous educational agency or institution attended by student</td>
</tr>
<tr>
<td>• College within the MCCCD system where the student has been enrolled</td>
</tr>
<tr>
<td>• Photograph of student</td>
</tr>
<tr>
<td>• E-mail address</td>
</tr>
</tbody>
</table>

Students who do not want directory information released may so indicate in writing either (a) during the admissions process or (b) by notifying the Office of Admissions and Records at every college at which they are enrolled.

Certain information is loaded into MCCCD’s learning management systems, such as the Instructure/Canvas-based Course Management System and RioLearn Learning Management System. As a result, examples of information visible to other students enrolled in the class may include: students’ names, official MCCCD e-mail addresses and enrollment in the class.

**Employee information:** Pursuant to the Arizona Public Records law, MCCCD Administrative Regulation 6.17 Requests for Public Information, and any other applicable rules and ordinances, the following are examples of information about present and former employees that may be disclosed without the employee’s prior written consent:

| • Name |
| • Titles or positions (including academic degrees and honors received) |
| • Fact of past or present employment |
| • Dates of employment |
| • Salaries or rates of pay |
| • Name of employee’s current or last known supervisor |
| • Disciplinary Records |
| • Self-Evaluations |
| • Performance Reviews |

Records that contain information about Personnel are not subject to release if they are works-in-progress or part of the deliberative process. Access to records that contain information about Personnel or disclosure of such information may be provided in compelling circumstances affecting the immediate health or safety of the individual and others.

**Other disclosures:** Under the Arizona Public Records Law, MCCCD may be required to provide information contained in MCCCD records to a third party. Commercial users may purchase public record information, such as non-confidential lists of students and employees. MCCCD may share aggregated information with governmental and non-profit agencies, and third-party vendors but only for legitimate educational and workforce development purposes.

**Opting Out**

As noted above, students who do not want directory information released may so indicate in writing either (a) during the admissions process or (b) by notifying the Office of Admissions and Records at every college at which they are enrolled.
Correcting Sensitive Information
As previously noted, if an individual wants to make any changes to information MCCCD receives from others about them, the individual must contact those sources.

Definition(s): As used in this administrative regulation, the following terms have the respective meanings set forth below:

ARS: Arizona Revised Statutes; the statutory laws that govern the state of Arizona as formally enacted in writing by the Arizona State Legislature, such as the Arizona law that requires businesses, including, but not limited to, colleges and universities, to provide consumer notification of data breaches involving personally identifiable information. Pursuant to ARS § 44-7501, “personally identifiable information (PII) (a) Means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable: (1) The individual’s social security number; (2) The individual’s number on a driver license issued pursuant to ARS § 28-3166 or number on a nonoperating identification license issued pursuant to ARS § 28-3165; or (3) The individual’s financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual’s financial account.” PII does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

FERPA: Family Educational Rights and Privacy Act; a federal law that protects the privacy of student education records. “Education records” are “those records, files documents, and other materials which 1) contain information directly related to a student; and 2) are maintained by an educational institution.” (20 U.S.C. § 1232g (a)(4)(A); 34 CFR § 99.3). FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

GLBA aka Financial Services Modernization Act of 1999: Gramm–Leach–Bliley Act; an Act that requires “financial institutions,” including, but not limited to, colleges and universities, to protect the privacy of their customers, including information that customers provide to a financial institution that would not be available publicly (“personally identifiable financial information (PIFI)”). MCCCD, therefore, has a responsibility to secure the personal records of its students and employees. To ensure this protection, GLBA mandates that all financial institutions establish appropriate administrative, technical and physical safeguards. GLBA also requires financial institutions to provide notice to customers about their privacy policies and practices, but institutions of higher education are generally exempt from this requirement, because they already do so under FERPA. Colleges and universities complying with FERPA are considered to be in compliance with GLBA.

HIPAA: Health Insurance Portability and Accountability Act of 1996; an Act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.
HIPAA Privacy Rule aka Privacy Rule: A statute that (1) establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, (2) requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization, and (3) gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information (PHI).” (45 CFR § 160.103). Individually identifiable health information” is information, including demographic data, that relates to:

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Ibid. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, social security number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

Payment Card Industry Data Security Standard (PCI DSS): Payment Card Industry Data Security Standard; a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, automated teller machine (ATM), and point-of-sale (POS/ePOS) cards. “Payment card information” is any personally identifiable information associated with a cardholder, such as the cardholder’s account number, account expiration date, name, address, or social security number. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered payment card information.

Personnel: All full-time, part-time and temporary employees and faculty who work for the MCCCD organization.

POI: Person(s) of Interest; individuals such as the following who are not considered part of the MCCCD workforce but who are still of interest to the organization:
<table>
<thead>
<tr>
<th>Person of Interest Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual enrollment instructor</td>
<td>Individuals who teach college-level courses to high students and are not compensated by MCCCD</td>
</tr>
<tr>
<td>Consultant</td>
<td>Individuals who are hired to do specialized work for MCCCD and are paid by outside sources</td>
</tr>
<tr>
<td>Agency temporary employee</td>
<td>Temporary agency employees who come to work for MCCCD and are paid by the temporary agency</td>
</tr>
<tr>
<td>Retired employee</td>
<td>Retired employees who continue a relationship with MCCCD are changed from Employee status to Person of Interest status</td>
</tr>
<tr>
<td>Call center or contract employee</td>
<td>Employees who provide support for some of our systems and are paid by the contracted company</td>
</tr>
<tr>
<td>Unpaid intern</td>
<td>An individual who is completing an internship at MCCCD for credit in their degree program</td>
</tr>
<tr>
<td>Volunteer</td>
<td>An individual who is working at MCCCD on a volunteer basis</td>
</tr>
<tr>
<td>Vendor (e.g., Follett bookstores, Chartwells dining services, Aramark facilities services)</td>
<td>Members of organizations that provide services to MCCCD employees and students</td>
</tr>
<tr>
<td>ESS Educational Services (e.g., hospitals providing adjuncts for nursing program and/or Fire Science/EMT department)</td>
<td>Members of organizations that have contractual relationships with MCCCD for specialized programs</td>
</tr>
</tbody>
</table>

**Security Incident:** The unauthorized access to and/or misappropriation of Sensitive Information.

**Sensitive Information:** Information that is so deemed under applicable law. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Sensitive Information covered under the Arizona Revised Statutes (ARS), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.

**Technology Resources:** MCCCD Administrative Regulation 4.4 Technology Resource Standards provides the following examples of technology resources: Websites, applications (such as, but not limited to, MCCCD’s Instructure/Canvas-based Course Management System and RioLearn Learning Management System), desktop and laptop systems, printers, central computing facilities, MCCCD-wide or college-wide networks, local-area networks, telephones, facsimile machines, scanners, access to the Internet, electronic mail and similar electronic devices and information.
AR 4.22 Statement on Privacy (cont’d)

Reference(s):
MCCCD Administrative Regulations 2.1 General Regulation, 2.5.1 Disciplinary Standards, and 2.5.2 Student Conduct Code
MCCCD Administrative Regulation 2.5.3 Student Records
MCCCD Administrative Regulation 3.8 MCCCD Institutional Review Board (IRB)
MCCCD Administrative Regulation 4.4 Technology Resource Standards
MCCCD Administrative Regulation 6.11 Identity Theft Red Flag and Security Incident Reporting
MCCCD Administrative Regulation 6.17 Requests for Public Information

Records Retention and Disposition Schedules for Arizona Community Colleges and Districts are located at: https://chancellor.maricopa.edu/public-stewardship(records-retention-and-disposition-schedules-for

Contact(s):
Pursuant to MCCCD Administrative Regulation 6.11 Identity Theft Red Flag and Security Incident Reporting, anyone who notices that a MCCCD technology resource(s) is currently being or may have been used in an inappropriate fashion should contact the Chief Privacy Officer via email at protectprivacy@maricopa.edu or by phone at 480-784-0PII (x 4-0PII or x 4-0744).

Please email info@domain.maricopa.edu with any questions and concerns about the MCCCD administrative regulations.

Please email protectprivacy@maricopa.edu with any legal questions and/or to arrange for the evaluation of any vendors, subcontractors and/or third-party products in advance of any work or purchase.

Amended by Direct Chancellor approval: November 12, 2014
Adopted by Direct Chancellor approval: June 19, 2014