

Guidelines for Collection, Use and Disclosure of Personal Information at MVC

Employees are expected to comply with laws and policies that apply to the collection or use of personal information and they are expected to take steps necessary to protect the privacy of all faculty, staff, and students.

In the course of District business, it is necessary to record, store, process and transmit personal information. The District and MVC takes its responsibilities with respect to the use of personal information seriously and seeks to provide functional and secure systems for the appropriate handling of this information.

Access: Student and employee private information may only be shared with individuals employed by the DCCCD, or its agents, who have a legitimate educational, business or supervisory interest in that information. See the table at the end of this brochure for private vs public information and the DCCCD web site for further definition:
<http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/>

Disposal: When personal information is no longer needed, and is not required to be maintained by law or as a Public Record, it should be disposed of according to DCCCD's approved policy. See Business Procedure Manual Section 19 - Records Management http://www.dcccd.edu/shared-nfs/intranet/dcccd/business_affairs/bpm/toc19.htm

Thorough shredding or recycling in appropriate secured containers is expected for all hardcopy documents. Destruction of information on computer disks and other magnetic media should be accomplished with an overwriting process. A simple "erase" process is not sufficient to completely destroy information and consequently enables inappropriate recovery and disclosure of information.

Off-Site: The requirements for handling of personal information are the same regardless of on or off campus location

Phones: The speaker on your phone should not be used when dealing with private information, a head/handset should be used. Remember that your voice may be heard by visitors and others who should not have access to confidential private data.

- Computers:** The display screens for all computers used to view private or sensitive data -- including personal information -- should be positioned such that they cannot be viewed by people who should not have access (e.g. through a window, from an adjacent hallway, or waiting areas, etc.)
- Printouts:** When handling documents containing private information, steps should be taken to safeguard the information from disclosure; including locking offices and storing under lock and key.
- Training:** Precautions should be taken when testing, or training on systems that contain personal information. In cases where the personal data is required, controls for access, security protection and erasure should be in place.
- Disclosure:** Private information about District employees, or students, should not be disclosed to persons or entities outside the District who do not meet the criteria of 'Handling of Personal Information,' unless permitted by law, or by prior written consent from District Legal.
- Web Pages:** With information systems utilizing the Internet and web browsers for processing activities, web page processes should adhere to and follow the same rules and policies that guide the activities for all information systems.
- Questions:** Please contact your location Information Privacy and Security Office if you have questions. A list can be found at the following District link:
<http://dsc3.dccd.edu/intranet/dccd/infosecurityprogram/IPSPCommittee/IPSOfficers.htm>

Information Security Private Vs Public Information

Private Information

The following is a compiled list of private information from various DCCCD information security sources.

Employee Information

- Social security number
- Birth date
- Home phone number
- Home address
- Health records
- Passwords
- Gender
- Ethnicity
- Citizenship
- Citizen visa code
- Veteran and disability status

Protected Patient Health & Research Identifiers

- Name
- All geographic subdivisions smaller than a state (street address, city, county, precinct) Note: zip code or equivalent must be removed, but can retain first 3 digits if the geographic unit to which the zip code applies if the zip code area contains more than 20,000 people.
- For dates directly related to the individual, all elements of dates, except year (date of birth, admission date, discharge date, date of death).
- All ages over 89 or dates indicating such an age, except that you may have an aggregate category of individuals 90 and older.
- Telephone number
- Fax number
- Email address
- Social security number
- Medical record number
- Health plan number
- Account numbers
- Certificate or license numbers
- Vehicle identification/serial numbers, including license plate numbers
- Device identification/serial numbers
- Universal resource locators
- Internet protocol addresses
- Biometric identifiers
- Full face photographs and comparable images
- Any other unique identifying number, characteristic or code.

Public Information

The following information is available to the public.

Employee Information

- Name
- Salary
- Gross pension
- Value and nature of fringe benefits
- Expense reimbursements
- Job titles
- Job description
- Education and training
- Previous work experience
- First and last employment
- Existence and status of complaints
- Terms of buy-out agreements
- Final disposition of disciplinary action
- Work location
- Work phone number
- Badge number
- Honors and awards received
- Payroll time sheets
- Employee ID
- University Email Address

Private Information

Non-directory Student Information

May not be released except under certain prescribed conditions.

Non-releasable information includes:

- Grades
- Courses taken
- Schedule
- Test scores
- Advising records
- Educational services received
- Disciplinary actions
- Student ID

Financial/ Credit Cards

- Any information obtained during the offering or delivery of a financial product or service that is identifiable to an individual such as:
 - Name
 - Address
 - Phone number
 - Account balances
 - ACH numbers
 - Bank account numbers
 - Credit card numbers
 - Credit rating
 - Location of birth
 - Driver's license information
 - Income history
 - Payment history
 - Tax return information
- Any information obtained during the processing of a credit card payment transaction that identifies individual consumers and their purchases, such as:
 - Account number
 - Expiration date
 - Name
 - Address
 - Social security number

Other

- Legal investigations conducted by the University
- Sealed bids
- Trade secrets or intellectual property such as research activities
- Location of assets
- Linking a person with the specific subject about whom the library user has requested information or materials.

Public Information

Student Directory information

The following information is Public, unless the student has requested non-disclosure (suppress).

- Name
- Address
- Electronic (e-mail) address
- Telephone number
- Dates of enrollment
- Enrollment status (full/part time, not enrolled)
- Major
- Adviser
- College
- Class
- Academic awards and honors
- Degree received

Financial/ Credit Cards

- Financial data on public sponsored projects
- Invoices and purchase orders

Other

- Course offerings