ROCHESTER
COMMUNITY AND TECHNICAL COLLEGE

SECURITY CAMERA ON CAMPUS
(RCTC Policy 5.24.5.1)

Part 1. Policy
Rochester Community and Technical College (RCTC) uses security cameras as one resource to enhance safety and security of persons and property. Additionally, security cameras may provide beneficial information for management and operations of RCTC. All security camera installations must be approved in advance by designated RCTC personnel, as described in this policy, except in the case of an emergency that makes such consultation impractical. Placement and use of security cameras must conform to applicable state and federal laws in addition to system and campus policies. Security cameras must not have audio monitoring or audio recording capabilities enabled. Video monitoring of public areas for security purposes must be limited to uses that do not violate the reasonable expectations of privacy of employees, students, and visitors, as defined by law.

Part 2. Scope
This policy applies to all personnel, students, and departments of RCTC in the use of its equipment for video surveillance, monitoring, and recording on RCTC-owned, leased, or controlled properties; this policy does not apply to the use of video applications for academic, research, or educational purposes of RCTC, or to security cameras installed by authorized financial institutions to monitor ATM machine usage on campus.

Part 3. Management and Use of Security Cameras
The primary purpose of security cameras is to assist in the daily operations of campus security and safety in providing a safe and secure environment to the RCTC community including students, employees, and visitors. Information obtained through video monitoring will be primarily used for security and law enforcement purposes. Information obtained through authorized surveillance may be used in support of disciplinary proceedings against RCTC personnel or students, or by RCTC for other appropriate management and operations decisions and related purposes such as litigation.

The installation and monitoring of security cameras and equipment must be administered by the Minnesota State employee designated by the president of RCTC in a manner consistent with this policy. For purposes of this policy the designees will be the Vice President of Facilities and Finance as well as the Director of Campus Safety and Security. The designee may authorize the use of video surveillance in a temporary location upon request of a college official if a specific safety or security risk exists; if the request concerns the investigation of individuals, the designee shall consult with the Office of General Counsel and/or human resources office of Labor Relations in the system office prior to approval. The designee shall consult with system legal counsel if requested by law enforcement to install video surveillance for a criminal investigation.

If concern over camera placement should arise, concerned persons may submit a petition to the designee for the removal or relocation of an existing camera. The designee will review petitions regarding camera location(s) and determine whether the policy is being followed. The designee will determine the appropriateness of an installation by weighing the concerns of the person(s) making the request and the safety and security of the entire community. The designee will weigh whether the potential increment in community security outweighs any likely infringement of individual privacy.

Part 4. Principles
The following principles shall apply regarding the use of security cameras at RCTC under this policy:

- All recording or monitoring of activities of individuals or groups by authorized RCTC security cameras will be conducted in a manner consistent with applicable system and RCTC policies, and will not be based on an individual's race, gender, ethnicity, sex, disability, or other personal characteristics that are protected by Board Policy 1.B.1.
- All recording or monitoring of video records will be conducted in a professional, ethical, and legal manner. Campus security and other personnel with authorized access to video recordings must receive a copy of this policy and will receive training on the effective, legal, and ethical use of the monitoring equipment upon assuming their role and at least annually thereafter.
- All recording or monitoring for security and safety purposes will be conducted only in areas where the public does not have a reasonable expectation of privacy. (e.g., not living spaces).
- Recorded images made by security cameras will be securely maintained by the RCTC pursuant to its records retention schedule. The alteration of video images is strictly prohibited.

Part 5. Limiting Use, Disclosure, and Retention of Recordings

The designee is responsible for controlling access to the security cameras monitors and recordings consistent with applicable privacy laws. Security camera data maintained by [College/University] may be nonpublic or private data on individuals under the Minnesota Government Data Practices Act and the Family Educational Rights and Privacy Act (FERPA). (Video surveillance data may be nonpublic or private "security information" as defined by Minn. Stat. § 13.37 Subd. 1 (a) or private personnel or educational data pursuant to Minn. Stat. §§13.43, Subd. 4 and 13.32, Subd. 3, and FERPA, 20 USC 1232g, which may be accessed, used, and disclosed to third parties only as consistent with those laws.)

Nothing in this policy shall prevent reporting to law enforcement real-time observations of conduct that appears to constitute criminal activity.

Recorded images will be stored in a secure location with access by authorized personnel only. A log must be created by the designee and maintained by authorized designee(s) of all instances of access to or use of surveillance records. The log must include the date and identification of the person or persons to whom access was granted.

Security camera data shall be maintained with appropriate security in accordance with the RCTC records retention schedule, and will then be destroyed in a secure manner, unless retained as part of a RCTC proceeding, a criminal investigation, a court proceeding (criminal or civil), grievance or arbitration proceedings or other use as approved by the designee or designee(s). The designee is responsible for securely retaining any surveillance data, including a video recording, which may be required for evidentiary purposes. If a copy of a recording is required for evidentiary purposes, campus personnel shall consult with the Minnesota State Office of General Counsel or the Attorney General's Office on protocols that may be required for authentication or other purposes and shall use a permanent storage device such as a CD, DVD, or USB drive and physically label the device with the date, time, and location of the recorded incident. No video footage segments or individual image copies, other than those required for system backup or evidentiary purposes, may be made, shared, or distributed without specific authorization/approval as stated above.

Part 6. Violations

Any individual who has concerns about the possible violation of this policy may discuss the matter with the designee. Any individual found to have violated this policy may be referred for discipline under the applicable personnel or student conduct process.

Individuals who are believed to have tampered with or destroyed security camera equipment or recordings, or individuals who have accessed security camera records without authorization, may be subject to discipline under the applicable personnel or student conduct process and criminal prosecution, as appropriate.

Date of Implementation: Immediately
Date of Adoption: 1/19/2022