RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

VIDEO MONITORING POLICY
Principles, Policy and Processes

POLICY PARTICULARS

DATE OF APPROVAL BY RELEVANT COMMITTEE STRUCTURE:
Finance & General Purposes (F&GP) Committee, Council

DATE OF APPROVAL BY COUNCIL: 22 June 2017

COMMENCEMENT DATE: June 2017

REVISION HISTORY: Policy finalised May 2017

REVIEW DATE: 5 year intervals

POLICY LEVEL: Administrative management

RESPONSIBILITY: Manager: Campus Protection Unit

REPORTING STRUCTURE: Manager: CPU; Deputy Director: Facilities Services; Executive Director: Infrastructure, Operations & Finance; Vice-Chancellor; F&GP; Council

1. PREAMBLE

Rhodes University allows the use of approved video monitoring systems through a transparent process, subject to rules governing equipment installation and deployment, and use of the resulting recorded material.

2. PURPOSE

Rhodes University aims to provide a secure environment for members of its community and to protect personal safety and property, assisted by video monitoring systems technology. Such technologies, however, must be used only to meet the university's critical goals for security in a manner that is sensitive to interests of privacy, free assembly, and expression.

3. PRINCIPLES

Rhodes University aims to provide its community with a secure environment, which is enhanced by using video monitoring systems (VMS) technology to monitor its campus. The University is also sensitive to the privacy and freedoms of expression and assembly of members of its community. As a result, this policy limits the use of approved equipment and the circumstances in which recorded material may be released. Furthermore, VMS technology is not intended to be used as a tool for routine performance management of university employees.

- **Note**: Violations of any aspect of this policy may lead to disciplinary, civil, or criminal action.
- **Note**: This policy and its provisions are not intended to prohibit University Audit or University Council, directly or through an agent, from conducting investigations that may include the engagement of monitoring systems.

This policy does not apply to legitimate academic use of cameras for educational purposes, to cameras used for journalism, or to private cameras owned and operated by members of the campus community.

4. UNIVERSITY VMS MONITORING POLICY

All video monitoring systems used on Rhodes University property are subject to this policy, whether they be the centralized system managed by CPU, or a localized stand-alone system.

A. CAMERA PLACEMENT:

The following guidelines apply to the placement of cameras on campus:

a. The CPU may establish temporary or permanent cameras in publicly accessible areas of the campus. These cameras may not make audio recordings.

b. Cameras may not be established in private areas of the campus. Private areas include residence rooms, bathrooms, shower areas, locker and changing rooms, areas where a reasonable person might change clothes, and private offices. Additionally, rooms for medical, physical, or mental therapy or treatment are private. Private areas also include the entrances, exits, lobbies, consulting rooms or hallways of the Counseling, Health and Wellness Center. The only exceptions are cameras used narrowly to protect money, documents, supplies or pharmaceuticals from theft, destruction, or tampering.
c. Cameras shall not be directed or zoomed into the windows of any private residential space or office. To the maximum extent possible, electronic shielding will be placed in the camera so that the camera does not have the capability to look into or through windows.
d. Cameras shall not be directed or zoomed into the windows of any private building not on University property.
e. Teaching venues shall not be monitored as part of normal daily security monitoring.
f. Should there be probable cause that lectures may be unduly disrupted, the video monitoring of teaching venues may be authorised by the VC (or in his/her absence one of the DVCs).
g. Examination and test venues will be monitored as part of the invigilation process, and to guard against any form of disruption of the assessment.

B. **CAMERA USE AND NON-USE:**

The following guidelines apply to camera use and non-use:

a. Cameras shall be used exclusively for campus safety purposes.
b. Monitoring cameras will not be used to evaluate employee performance unless a formal investigation results in a determination that a safety issue may exist.
c. Cameras will not be used to monitor individual students, faculty, or staff, except as necessary for a criminal investigation and except as in accordance with the terms of a warrant. Cameras may be used to monitor a student or employee work area, such as an area with financial transactions, even if there is only one student, faculty, or staff member employed in that work area. Cameras used to monitor a work area are not intended to view the contents of computer screens, and may not be used to monitor computer usage.

C. **ESTABLISHMENT OF CAMERAS ON CAMPUS:**

a. Temporary cameras are defined as cameras that are established by the CPU to provide additional security for a campus event or situation

and that are not in place for more than 30 days. Permanent cameras are established as part of the campus infrastructure.

b. The Executive Management Team of the University in consultation with the Head of CPU shall determine placement and use of cameras. Other departments, committees or individuals may recommend placement of cameras.

c. Legitimate safety and security purposes include, but are not limited to, the following:

- Protection of individuals on university property.
- Protection of buildings and property.
- Building perimeter, entrances and exits, lobbies and corridors, elevators, receiving docks, special storage areas, laboratories, cashier locations, etc.
- Monitoring and recording of access control systems.
- Monitoring and recording restricted access transactions at entrances to buildings and other areas.
- Verification of security alarms.
- Intrusion alarms, exit door controls, panic buttons, etc.
- Electronic patrol of publicly accessible areas.
- Transit stops, parking lots, public (enclosed and unenclosed) streets, vehicle intersections, etc.
- Criminal investigation.
- Robbery, burglary, and theft monitoring.
- Monitoring of pedestrian and vehicle traffic and vehicles in traffic areas at intersections.

D. **CAMERA MONITORING:**

a. Images and recordings may only be monitored by authorized CPU staff, members of Executive Management, staff with responsibility for residence hall security, persons responsible for adjudication of campus code of conduct violations, and other officials as authorized by the Vice Chancellor (or one of the DVCs in his/her absence). No students may be hired to monitor recordings or images. Staff responsible for installation and maintenance of monitoring equipment may access recordings only to the extent necessary to carry out their duties.

b. Those officers and authorized staff approved for monitoring will receive training in effective, legal and ethical use of the monitoring equipment. These officers and authorized staff will receive a copy of this policy and provide written acknowledgement that they have read and understand this policy. Officers and authorized staff will receive any and all updates or amendments to this policy.

E. **STORAGE MEDIA:**

a. Recordings will be stored in a manner consistent with available technology and transported in a manner that preserves security. Current and archived recordings shall be kept locked and secured.
b. Current and archived recordings under review by authorized officials shall be subject to a process where the recordings are signed in and out in a logbook.
c. Footage relating to an alleged incident shall only be passed to an investigating agency external to the university or the SAPS by the Manager: Campus Protection Unit, or an equivalent officer of the university specifically authorised, after authorisation by the VC or in his/her absence one of the DVCs.
d. Recordings not related to or used for an investigation will be kept strictly confidential and overwritten within 60 days. Recordings or images used for investigation or prosecution of a crime shall be retained until the end of the court or judicial proceedings and appeal period unless directed otherwise by a court of law.
e. No attempt shall ever be made to alter any recording. Editing or otherwise altering recordings or still images, except to enhance quality for investigative purposes or blur features to protect privacy, is strictly prohibited.
f. Transmission of recordings using the internet or campus network will use encryption technology to ensure that recordings are not improperly accessed. CPU will work with the I&TS staff to establish security for the system and to ensure proper password and encryption technology for recordings or images transferred or transmitted over the internet or on the campus network.

F. **DESTRUCTION OR TAMPERING WITH VMS EQUIPMENT:**

Any person who tampers with or destroys a camera or any part of the electronic monitoring system may be prosecuted in the criminal justice system as well as the campus judicial system.
