योजना एवं वास्तुकला विद्यालय, भोपाल

राष्ट्रीय महत्व का संस्थान, शिक्षा मंत्रालय, भारत सरकार

School of Planning and Architecture, Bhopal

An Institute of National Importance, Ministry of Education, Government of India

CCTV POLICY GUIDELINES

INDEX

SCHOOL OF PLANNING AND ARCHITECTURE, BHOPAL

(An Institution of National Importance, Ministry of Education, Govt. of India)

CCTV POLICY GUIDELINES

1. Objective

School of Planning and Architecture (SPA) Bhopal is committed to enhancing the safety of the campus by integrating campus safety and security through CCTV installation and monitoring. The Video monitoring and recording will be conducted in a professional, ethical, and legal manner that should respect the reasonable expectation of privacy among all members of the campus. This policy concerns the installation and use of CCTV to monitor and record areas for the purposes of safety and security of the School of Planning and Architecture (SPA), Bhopal. The purpose of CCTV system installations aims to ensure:

- Campus security and safety
- Protection of institutional assets
- Respect for individual privacy
- Compliance with legal and regulatory requirements

2. Scope

This policy is applicable to all students, faculty, staff, campus residents, vendors, contractors, and other visitors of SPA Bhopal including coverage of surrounding public areas (*e.g.*, main approach roads, market areas just outside the campus shared boundaries). This policy does not address the use of recording equipment for educational or research purposes such as, experiments or projects, lectures, interviews, concerts, athletic events, plays, or other public performances. Such recording may be subject to other policies governing research with human subjects and academic, privacy and event-specific policies, as well as applicable to state and local laws. This policy is not intended to create any contractual rights.

3. Purpose and Use of CCTV

Cameras used for CCTV shall be installed after approval of competent authority of SPA Bhopal in consultation with estate and security office and other concerned. CCTV may only be used to monitor and record for legitimate safety and security purposes including, but not limited to, the following:

i. *Criminal offense:* Robbery, assault, theft surveillance, etc.

ii. *Monitoring of public areas:* Transit stops, parking lots, public streets near campus, bike racks, University artwork and sculptures, etc.

iii. *Protection of buildings and property:* Building perimeters, cashier locations, and entrance and exits of lobbies and corridors, receiving docks, special storage areas, laboratories, etc.

iv. *Verification of security alarms:* Intrusion alarms, exit door controls, etc.

v. *Monitoring of access control systems:* Restricted access transactions at entrances to buildings and other areas

vi. *Protection in highly sensitive laboratory environments:* Laboratories containing materials or hosting activities that are highly sensitive or dangerous and thereby raise health, safety and/or national security concerns

vii. *Compliance with government requirements:* Pursuant to laws and other government requirements pertaining to public safety and security.

4. Location and coverage of CCTV surveillance

The CCTV cameras can be installed at following location and it will have area under surveillance and areas under prohibition as listed below

S.N.	Location	Areas under surveillance	Prohibited Area
1a	Academic Buildings interior space	Entrance, Waiting areas, Stairs, Lift Lobby, Class rooms, Studios, Corridors, Courtyards, Various Labs, Workshop, Seminar Halls, Conference room, Shared public/ Interaction spaces, etc	Faculty rooms, Toilets, Girls common rooms, Sick room, etc.
1b	Academic Buildings outer space	Entry gates, open green and paved passage, Outer perimeter of buildings, Terraces, Parking lots, Recreation spaces around buildings.	Camera should not capture inside view of areas listed under prohibition
2a	Students Hostels interior spaces	Entrance, waiting areas, Stairs, Lift Lobby, Corridors, Courtyards, Shared Interaction spaces, Recreation Hall, indoor game hall, Dining hall, Visitors room, cooking areas, Utensil washing areas, etc	Students' rooms, Toilets, Girls common rooms, Sick room, warden room, Balconies, etc.
2b	Students Hostels outer spaces	Entry gates, open green and paved passage, Outer perimeter of buildings, Terraces, Parking lots,	Camera should not capture inside view of areas listed under prohibition

		Recreation spaces around buildings.	
3	Admin Buildings Estate office, Data centre	Entrance, waiting areas, Stairs, Lift Lobby, Corridors, Courtyards, common working spaces, Pantry, Seminar Halls, Conference room, etc	Individuals' rooms, Toilets, etc.
4	Research Centres, Examination, Admission centre, Library, etc	Entrance, waiting areas, Stairs, Lift Lobby, work stations, Reading rooms, book stacks, Corridors, Various Labs, Workshop, Seminar Halls, Shared public/ Interaction spaces, etc	Individuals' rooms, Toilets, confidential sections, etc.
5	Service buildings	Electrical Sub-Stations, Control panels, Water storage tanks, sewer treatment plant, SWM Site, etc.	Individuals' rooms, Toilets, etc.
6	Entry/Exit gates, Roads and Parking	Entry and Exit gates of the campus, Road intersections, Parking lots, campus roads, pathways, etc.	Individuals' rooms, Toilets, etc.
7	Public Buildings	Premises of Canteen, Bank, kiosks, convenient shops, stationery and printing shops, Indoor sport halls, etc.	Individuals' rooms, interior spaces, Toilets, etc.
8	Public open Spaces	Play fields, OAT, Gardens, Parks, Open Gymnasium, Children play area, Restricted	NA

		Areas such as Ponds, swamps, reserved green, dangerous slopes/ depressed areas, hills, etc.	
9	Site surroundings	All along the campus boundary walls, Areas have soft /Brocken boundaries, Main approach road of Campus, Market areas just along the campus	NA
10	Guest house, Faculty and staff residential areas	Outer premises of the buildings may be captured to identify public movements around these areas including parking lots and common activity areas, institute club, Community halls, etc.	Camera should not capture inside view of residential private areas, toilets,

4a. Exceptions

i. The prohibitions in the locations listed above refer to camera installations that would not allow the surveillance of the interior and view from outside of the designated locations. For example, the policy does not allow the installation of cameras in a private room of faculty, staff and hostel room of the students but, in case of special circumstances that may have valid reasons, competent authority may allow surveillance for specific time duration.

ii. Generally, Cameras will be installed in locations that are open and conspicuous and will not be activated or configured to record audio but, in case of special circumstances that may have valid reasons, competent authority may allow audio recording of a particular camera.

iii. In situations involving threats to the safety of the campus, to the life, health or safety of any person, or of theft or destruction of property and upon consultation with the competent authority, temporary exceptions may be made to the prohibitions in the list given above.

iv. However, individuals' rooms are prohibited for general surveillance but, in case where an individual makes a personal request to monitor their own room the competent authority may accept/reject such request.

v. Departments, programs, centres, or any affiliates of the SPA Bhopal wishing to change, install new, or expand CCTV camera coverage may submit a request for consideration. As applicable, the request should include (1) a description of the safety, security, or other issue warranting the change or installation of the camera(s); (2) proposed location of the camera(s) to be installed; and (3) funding source(s) for initial installation of the equipment and ongoing annual maintenance.

5. Maintenance of CCTV Data through centralized system

a) All CCTV footage will be stored on centralized servers managed by the Computer/Data Center (CDC) of the institute who will ensure data backups on a regular basis to ensure data security and redundancy.

b) Data from CCTV (*e.g.*, surveillance footage) is maintained consistent with the storage capacity of 30 days or as per prevailing government guidelines (*e.g.*, many storage devices are automatically overwritten after 30 days, although this varies). Computer/Data Center (CDC) may use cloud storage for long-term archival storage.

c) CCTV data will be otherwise preserved for longer periods pursuant to a lawful order, in connection with litigation or potential litigation, or as part of institute or governmental investigation or an agency or court proceeding (criminal or civil).

d) CCTV may only be accessed and/or used by authorized personnel appointed by the competent authority. It may be shared with other authorized persons after approval of the competent authority on a need-to-know basis only.

e) Authorized person (s) from the computer/data centre will take necessary steps to make the CCTV system in working condition by regular maintenance and upgradation of hardware software and networks as per institute procurement rules.

f) For regular maintenance and upkeep of the CCTV system, an Annual Maintenance Contract (AMC) shall be established with a qualified service provider to handle repairs, software updates, and performance checks. The terms of the AMC should cover response time, resolution of issues, and periodic system inspections.

6. Access to CCTV footage through Decentralized system

a) Access to CCTV footage for monitoring purposes a decentralized system can be adopted in which various departments may authorize specific personnels with limited and controlled access for monitoring only.

b) In principle, responsibility for the campus wide safety and security lies with the estate and security office appointed by the competent authority for this purpose. Arrangement should be made for 24x7 monitoring of footage by the estate and security officer.

c) Limited and controlled Access (right to see only) to monitor CCTV Footage of hostels may also be given to the concerned Chief warden and wardens. Hostel Care takers and security guards may help in monitoring.

d) Departmental heads and centre heads may request competent authority for granting controlled access (right to see only) to monitor specific parts of their working area such as, Labs, studios and workshops, etc.

7. Sharing of CCTV data

CCTV data will be treated sensitively and will not be shared outside of the institute except following situations:

a) To authorized agencies (*e.g.*, Police, attorneys or insurance providers) on a need-to-know basis after the approvals of the competent authority,
b) Subject to a lawfully issued or court order, or
c) As needed to law enforcement or other public officials in the case of an emergency situation involving threats to the safety of the campus, to the life, health or safety of any person, or of theft or destruction of property. Notwithstanding the foregoing, distribution of CCTV data through Clery Crime Alerts and equivalent warnings are permitted use.
d) CCTV data records will be in control of the person authorized by the competent authority of SPA Bhopal
e) The right to download recorded data for sharing with others including outside agencies would require written permission along with appropriate directions from the competent authority of SPA Bhopal. Such requests should be routed through a proper channel.

8. Responsibilities

a. Estate and security office (ESO) of SPA Bhopal

- In principle, ESO will be the authorized office to have full administrative rights to CCTV monitoring; however, data storage and system maintenance would be carried out by the central computer/data centre. All CCTV data will be stored in a secure location with access by authorized personnel only.

- The Director SPA Bhopal may authorize personnel from the institute, departments, specific centres, computer/data centre and the security office with rightful access to CCTV data.
- Authorized personnel will be trained in the technical and ethical parameters of appropriate CCTV access and use. Routine maintenance checks for CCTV must be conducted by the ESO
- All the personnel that have access to CCTV monitoring will provide written acknowledgment that they have read and understood CCTV policy documents.
- ESO will be responsible for the overall CCTV operations, including installation and maintenance of cameras. However, ESO may take technical help from computer/data centres and stores and purchase sections for regular maintenance and replacement of CCTV cameras and cables, etc.
- ESO will be responsible for ensuring compliance with campus safety and security norms applicable to higher education institutions and data protection laws amended from time to time.
- ESO will be responsible for coordinating with the agencies requesting CCTV footage for legal and administrative use in compliance with relevant laws. An ESO or Authorized person from the ESO office will facilitate the sharing of CCTV data to requesting agencies as per guidelines provided at para-7 of this policy document.
- The ESO will maintain a log of shared CCTV data. The log will include personnel names and titles, reason(s) the CCTV data was sought, time/date/location provided, who authorized the access, any further use or distribution of data, and affirmation that the personnel understand their obligation to perform duties in accordance with this policy.

- ESO will consult with the competent authority of SPA Bhopal upon receipt of a legal request or court order for obtaining CCTV data from SPA Bhopal campus.

b. Responsibilities of Computer/Data Centre (CDC)

- Computer/Data Centre (CDC) of SPA Bhopal will manage and maintain centralized storage infrastructure, software, hardware including servers and backups.
- Computer/Data Centre (CDC) of SPA Bhopal will assist the office of Dean Planning and Development for installing basic infrastructure, network cables, CCTV cameras etc.
- Computer/Data Centre (CDC) of SPA Bhopal will be responsible for Enforcing system access controls and security configurations.
- Computer/Data Centre (CDC) of SPA Bhopal will be responsible to Conduct regular audits to ensure compliance with this policy.
- Computer/Data Centre (CDC) of SPA Bhopal will be responsible to look into technical troubleshooting, network issues and will approve the access permissions to the persons authorized by the competent authority of SPA Bhopal.
- Computer/Data Centre (CDC) of SPA Bhopal will be responsible to ensure network quality of service and all technologies related to network connectivity, bandwidth and security planning, including applying best practices to meet the demands and expectations of the system, physical security, and applying security to ensure the CCTV system is best protected from unnecessary interruption and/or intrusion.
- All user activities, including live feed viewing, playback, and system changes, should be logged and audited regularly by CDC.

- In case of planned or sudden system down for maintenance CDC will notify stakeholders
- CDC will ensure continuous CCTV recording. In the event of a system failure, local storage devices may be used to record footage as a temporary measure.

c. Responsibilities of Local Monitoring teams

Local monitoring teams includes following teams:

1. Security personals of ESO involved in campus wide safety and security
2. Wardens, Security personals and caretakers appointed at hostels
3. Personnels authorized and appointed by department heads for monitoring

- Local monitoring teams are responsible for real-time surveillance within their respective designated zones.
- Respond to alerts or incidents and report to the ESO for necessary actions.
- Report faults and operational issues to the CDC or ESO
- Assist in retrieving footage for investigations or legal purposes if required.

9. Legal Framework and Acts

The CCTV system must adhere to the prevailing legal guidelines and Acts such as,

1. **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011** under the Information Technology Act, 2000 in which it is highlighted that All CCTV footage must be stored securely, with encrypted access and defined retention periods.

2. **Right to Privacy under Article 21 of the Constitution of India** in which it is highlighted that CCTV monitoring must respect individual privacy rights, particularly in areas considered private.
3. **Indian Penal Code (IPC), Section 66E – Punishment for Violating Privacy** in which it is highlighted that All personnel must ensure that CCTV data is used exclusively for authorized purposes, and misuse can result in legal action.
4. **Surveillance Guidelines by the Ministry of Home Affairs (if applicable)** in which it is highlighted that CCTV installations must comply with national regulations on security, data protection, and monitoring practices.
5. **Data Protection Laws (e.g., GDPR or other applicable local regulations)** in which it is highlighted that compliance with data protection regulations must be ensured, especially for institutions with international students or staff.

10. Other

1. There shall be a CCTV Governance Panel which will consist of individuals representing the following offices:
    1. Directorate,
    2. Registrar office (Accounts & finance, store & purchase)
    3. Estate and security office
    4. Computer/ Data centre
    5. Office of Dean Academics
    6. Office of Dean Planning and Development,
    7. Office of Dean Student Affairs,
    8. Office of Dean Faculty/staff welfare
    9. Legal Advisors
    10. Special invitees (Centre Heads)
    11. Campus residents' representatives

2. The Panel will meet at least once annually to receive reports from ESO on CCTV practices and to ensure appropriate implementation of this policy. The reports will include information as requested about CCTV usage, including new or changed camera locations; access logs; community requests and all complaints or concerns; policy exception summaries; and other updates and developments.
3. The CCTV Governance Panel will review this policy periodically and recommend revisions if needed.