European University Cyprus

6 Diogenes Street, 2404 Engomi, Nicosia
P.O.Box 22006, 1516 Nicosia, Cyprus
**T:** 22713000, **E:** info@euc.ac.cy
**www.euc.ac.cy**

EXCELLENT

# CCTV Policy

## 1. Introduction

1.1 The European University Cyprus (EUC) is committed to providing a safe and secure learning environment across its campuses and buildings. The University therefore operates close circuit television cameras (CCTV) across its campuses and buildings for the security and safety of its staff, students and visitors.

1.2 Closed Circuit Television (CCTV) cameras are installed to view and record the areas, visibly at selected locations on University premises. The deployment of these cameras are a strategic component of the University commitment to staff and student safety, security and crime prevention.

1.3 The University's use of CCTV is covered by the General Data Protection Regulation (GDPR). Identifiable imagery is considered as personal data under the GDPR and, therefore, this policy is committed to the protection of individuals' rights and privacy. The processing of personal data such as the collection, recording, use, and storage of personal information through the CCTV system will be dealt with lawfully and correctly in accordance with the University's Data Protection Policy.

## 2. CCTV System

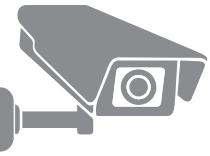
2.1 CCTV (closed-circuit television) is a TV system used for surveillance and security purposes at the entrances of EUC buildings (including floors' entrances, parking, high-risk areas (i.e. cashier)). CCTV does not monitor employees while they are working but it is only used for recording entry, exit and common areas traffic of individuals and students.

2.2 In no case the CCTV system can or it will be ever used to check the personal behaviour, personal contacts and efficiency of the individuals. This is against the freedom of individuals and against our Data Protection Policy.

## 3. Purpose of the CCTV System

3.1 **The purpose of the CCTV system is as follows:**

- To enhance Safety, Security and Crime Prevention on University premises.
- Safety of staff, students, contractors and visitors.
- Provide an effective means by which to prevent, detect and reduce crime in the monitored areas by offenders.
- Assist in the factual, accurate and speedy reconstruction of the circumstances of incidents.
- To assist the University and police in providing a swift response to criminal activity and provide evidential material for court and disciplinary proceedings.
- Protect the University assets.





- To assist in traffic management within University car parks.
- To assist in supporting University Health and Safety policies.
- To assist in the event of an emergency or disaster.

## 4. Scope

4.1 The CCTV system is intended to view, monitor and record areas within University premises. It will only record entrances and exit of EUC buildings including floors' entrances, parking areas, outside of elevators and high risk areas (cashier registry).

4.2 Every possible effort has been made in the planning and design of the CCTV system to give it maximum effectiveness. However it is not possible to guarantee that the system will see every single incident taking place inthe areas of coverage.

4.3 The CCTV system must strike an appropriate balance between the personal privacy of individuals using the campuses/buildings and the objective of recording incidents.

4.4 The system will be operated fairly to ensure that all CCTV data is processed in accordance with GDPR 2016/679, the Data Protection Act N. 125(I)/2018 and the University Data Protection Policy and only for the purposes to which it is established.

4.5 The system is not intended to invade the privacy of any individual in business or other private premises, buildings or land not belonging to the University.

4.6 No sound will be recorded in public places and CCTV is not used to record conversations.

4.7 No images will be captured in areas where individuals would have an expectation of privacy (for example; toilets, inside of elevators, showers, changing facilities etc.).

## 5. Signage

5.1 Strategically placed CCTV camera notices at key entry points to University premises will advise individuals that they are entering an area which is covered by CCTV cameras.

5.2 **The CCTV notice at entrances to the University and in adjacent areas will contain:**

- That there is a CCTV in place,
- The name of the Data Controller (European University Cyprus)
- The purpose (Safety & Security)

## 6. Data Protection

6.1 This policy document will be implemented to ensure that the deployment and control of CCTV resources is proportionate and lawful under the terms of the General Data Protection Regulations (GDPR 2016/679), the Data Protection Act N. 125(I)/2018 and the CCTV Codes of Practice issued by the Office of the Commissioner for Personal Data Protection of Cyprus.

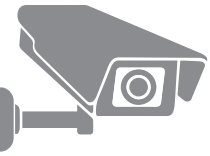
6.2 In summary, personal data should be processed in a manner that ensures its security and only if there is no less intrusive way to achieve the purpose(s). This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are in place.

6.3 The lawful basis identified for processing the personal data as part of the CCTV system is legitimate interests.

## 7. Assessment of the Policy

7.1 **The Head of Health & Security will evaluate the system periodically to consider the following:**

- The assessment of impact upon crime
- Assessment of areas without CCTV
- The views of the users
- Operation of the policy
- Whether the purposes for which the scheme was established still exist





- Future functioning, management and operation of the system

## 8. Management and Access to the CCTV System

8.1 The Department of Information Systems & Operations of EUC is responsible for the management of the University's CCTV system.

8.2 Eventually only an authorised employee (IT specialist) of the Department of Information Systems & Operations has access to the CCTV footage. CCTV footage is accessed and reviewed by the authorised individuals only when instructed by the Director of the Department of Information Systems & Operations and only after an incident and not at a constant basis.

8.3 After incidents and or investigations CCTV footage may be shared on a need-to know basis to the necessary technical staff and the appropriate Directors of EUC, DPO and Health & Safety Officer for the purpose prevention, investigation or detection of crime and /or the monitoring of the security and safety of the premises at the University.

8.4 All reported abuse or inappropriate use of the CCTV system will be investigated and if proven, the University will take appropriate measures to eliminate or minimize the risk of reoccurrence. Inappropriate use of the CCTV system will be considered a breach of University policy and will be handled accordingly.

8.5 All CCTV recording equipment will be located within secure areas and only accessible to authorised personnel.

## 9. Recording and Storage of Information

9.1 All recorded material will be treated as confidential and unless required for evidence, will be kept in accordance with this policy.

9.2 The CCTV systems are operated and monitored 24 hours a day, every day of the year.

9.3 CCTV images not to be retained for longer than necessary. Data storage is automatically managed by the CCTV digital recorders which use software programme to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces a miximum of 30 days rotation in data retention.

9.4 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal or disciplinary proceedings), the images will be erased following the expiration of the retention period.

9.5 If CCTV images are retained beyond the retention period, they will be stored in a secure place with controlled access and erased when no longer required.

9.6 Access to the CCTV System and to the captured images will be restricted to authorised staff involved in monitoring or investigation.

## 10. Access and Disclosure of CCTV Images

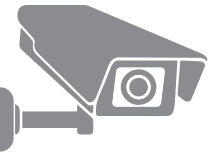
10.1 Requests for access to (review), or disclosure of (i.e. provision of a copy), of images recorded on the CCTV systems from third parties (i.e. unauthorised persons) will only be granted if the requestor falls within the following types of person / organisation:

- Data Subjects (i.e. persons whose images have been recorded by the CCTV systems)
- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution agencies (including University Managers in the course of Staff or Student disciplinary proceedings)
- Relevant legal representatives of data subjects

10.2 Images will only be released to the media and other parties on the authority of the University Board and following advice from law enforcement agencies to support police investigations.

10.3 Right of Access: Staff, students, visitors and other data subjects about whom the University holds or uses personal data have a legal right to access that information and request a copy of the data in permanent form. Any person wishing to exercise their right of access formally should complete the "Data Subject Access Form" and submit it along with proof of identity to prevent unlawful disclosure of personal data to: https://euc.ac.cy.

10.4 By law, the University has one month from receipt of the request along with proof of identity, in which to respond





to subject access requests. In any event the University will endeavour to respond as quickly as possible. In limited circumstances, the University may not be able to release personal data because exemptions under the Legislation are applicable, or the disclosure of the data would release personal data relating to other individuals.

10.5 Where a third party is acting on behalf of a data subject, written authorisation from the data subject must be provided to confirm that the third party is acting on their behalf.

10.6 The University has discretion to refuse any third party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once an image has been disclosed to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with the Data Protection Legislation in relation to any further disclosures.

10.7 It may be necessary for redaction of images on copies of CCTV issued following a subject access request. This is usually to protect third party data. Where redaction is deemed impossible for example big video files, the university may refuse a CCTV data request if providing this data infringes on the rights to privacy of others.

10.8 All disclosed CCTV data must be safely delivered to the intended recipient ideally by handing over information on a sealed data disc or other media storage device with encryption embedded in the CCTV application software. CCTV recorded data should not be transmitted by email.

10.9 Only the University Board along with the Head of Security and the DPO can authorise the viewing or release of CCTV data.

## 11. Liaison with the Police Services

11.1 Images may be released to the Police Service or other law enforcement agencies in compliance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR 2018) with the approval of the Commissioner for Personal Data Protection of Cyprus.

11.2 All CCTV data viewed or released to the police must be logged in the EUC compliance platform. Visiting police officers must provide their standard issued badge as proof of identity and provide signatures for any CCTV collected.

## 12. Installation

2.1 The CCTV installations are carried out through consultation with external CCTV providers (AV Solutions) approved by EUC. Personal data are not shared or intended to be shared with any providers or vendors.

12.2 Any technological change, which will have a significant effect upon the capacity of the system, will be fully assessed in relation to the purpose and key objectives of the system.

12.3 The University reserves the right to deploy/restrict/cease the use of dummy cameras as part of the system subject to applicable laws, Commissioner for Personal Data Protection of Cyprus directive or police directive.

## 13. Complaints

13.1 All complaint and enquiries relating to the CCTV system should be addressed to: Data Protection Officer of EUC at: **dpo@euc.ac.cy**

## 14. Breaches of the Code

14.1 Breaches of the policy and of security will be investigated by the Head of Security or the Data Protection Officer. Recommendations and corrective action plans will be put in place to remedy any breach which is proven.

14.2 The University Data Protection Officer are responsible for maintaining a record of CCTV data breaches as part of the policy.

## 15. Access Request Form

15.1 Under the General Data Protection Regulation (GDPR) you are entitled to request the personal data that we hold about you. Please use the form available on the University website **euc.ac.cy** to specify the data that you wish to access. Under GDPR we have one month in which to respond to you.