CCTV Policy			
Current Status:	Operational – Awaiting Approval	**Last Review:**	November 2023
Policy Owner:	Group Director of Compliance	**Next Review:**	March 2025
Roles Responsible for Review:	Group Director of Estates Group GDPR and Compliance Lead	**Originated:**	November 2021
Approved by:	SET Resources	**Committee:**	
Type of Policy:	Staff / Students / External	**Quality Assured by:**	

1. General/Summary

1.1. The purpose of this policy is to regulate the use of Closed-Circuit Television (CCTV) to monitor and record on campus for the purposes of safety and security. This policy applies to all personnel and property of the College in the use of CCTV monitoring and recording.

2. Aims

2.1 West Suffolk College has in place a CCTV surveillance system and "the system" operates within the perimeters of the Sixth Form Campus, The University Campus, and WSC's Leisure Learning Centres. Images are monitored and recorded centrally and will be used in strict accordance with this policy. The system is owned by West Suffolk College and is managed by the Estates Department.

2.2 The Estates Department has overall responsibility for the operation, maintenance, servicing, and inspection of the system ensuring compliance with this policy and that its procedures are documented. They may be contacted as follows:

Estates Department on Extn. 6550

The IT Services Team are responsible for system access and software updates as and when necessary. They may be contacted as follows:

IT Services Team on Extn. 6555

General Data Protection Regulations: CCTV digital images, if they show a recognisable person, are personal data and are covered by the UK General Data Protection Regulations UK GDPR). This Policy is associated with the College's Data Protection Policy, the provisions of which should be adhered to at all times.

3. The system

3.1 The system comprises of 118 internal & external fixed position cameras located remotely across the campus interlinked through encrypted network drivers such as: AXIS, VISTA & VIPER. Recording equipment is centrally located in secure server rooms with limited access and is password protected. Passwords are assigned to individual users and not shared in accordance with the colleges IT security policies.: User access onto the system is limited to 2 x IT and 1 x Estates Team member who are able to view and interrogate the data contained captured.

3.2 Cameras will be located at strategic points on the main campus, principally at the Access Roads, Classrooms, Edmund ITC, Grass Quad External, Leonardo External, at the Milburn Centre, Suffolk House external, Suffolk House internal, the Gateway and at West facing external and internal points. No camera is hidden from view. A list of locations is held by the Estates Team and Group GDPR and Compliance Lead.

3.3 Signs will be prominently placed at strategic points and at entrance and exit points of the main campus to inform staff, visitors, and members of the public that a CCTV installation is in use.

3.4 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

4. Purpose of the system

4.1 The system has been installed by West Suffolk College with the primary purpose of reducing the threat of crime generally, protecting the College premises and helping to ensure the safety of all College staff, students, and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension, and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/events which might warrant disciplinary proceedings being taken against staff and assist in providing evidence to managers and/or to a member of staff against whom disciplinary action is being taken or is threatened to be taken.
- Facilitate the movement of vehicles on site.
- In the case of staff to provide management information relating to employee compliance with contracts of employment.

The system will not be used:

- To provide recorded images for the world-wide-web.

- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

4.2 **Covert recording**

Covert cameras may be used under the following circumstances on the written authorisation or request of the DPL (Data Protection Lead) and where it has been assessed re: UK General Data Protection Regulations by the DPO Centre.

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

4.3 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

4.4 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

5. Monitoring of images

5.1 Images captured by the system will be recorded within the main campus server rooms, twenty-four hours a day throughout the whole year. Monitors are sited in the IT Services Department and the office of the Facilities Manager and are not visible from outside these rooms.

5.2 No unauthorised access to the recording system will be permitted at any time. Access will be strictly limited to the IT Services and Facilities Management Teams, police officers and any other person with statutory powers of entry. A list of those members of staff authorised to access the Control Room is maintained by the Data Protection Lead (DPL).

5.3 Staff, guests and visitors may be granted access to the system recording locations on a case-by-case basis and only then on written authorisation from the DPL. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter.

5.4 Before allowing access to the system recordings, a senior staff member should satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, located in the office of the Facilities Manager which shall include details of their name, their department, or the organisation they represent, the person who granted authorisation and the times of entry to and exit from the control room. This will also include any visitors granted emergency access. Only the Facilities Manager will issue any footage, supported by the IT Team who may download the required footage only then on written authorisation from the DPL.

6. Staff

6.1 All staff working in the IT Services and Facilities Management Teams will be made aware of the sensitivity of handling CCTV images and recordings. The DPL will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

6.2 Training in the requirements of the UK General Data Protection Regulations and/or The Data Protection Act 2018 will be given to all those required to work in the IT Services and Facilities Management Teams by the DPL.

7. Recording

7.1 Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

7.2 Images will normally be retained for a 1 Month period from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

7.3 If footage is exported this is kept for no longer than 3 months unless footage is required to be kept longer than this due to exceptional circumstances, i.e., a court case.

7.4 All hard drives and recorders shall remain the property of West Suffolk College until disposal and destruction. Destruction will take place in the form of drive physically destroyed by an approved external provider that provides a data blanking/removal service and certification.

8. Access to images

8.1 All access to images will be recorded in an Access Log.

8.2 Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system. A list of such staff is held by the Data Protection Lead (DPL).

8.3 Access and disclosure to images/recorded material by third parties, will only be allowed in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime. We will carry out a Legitimate Interest Assessment for each request of this type before any footage is released.
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.

- Emergency services in connection with the investigation of an accident.

8.4 Access to images by a data subject

CCTV digital images, if they show a recognisable person, are personal data and are covered by the UK General Data Protection Regulations and The Data Protection Act 2018. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Regulations. They do not have the right of instant access.

8.5 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the DPL. Subject Access Request Forms are obtainable in hard copy from the DPL. An electronic copy can be obtained by email request to the **dpl@wsc.ac.uk**.

8.6 The DPL will then arrange for a copy of the data to be made and given to the applicant, once the requestor's ID has been verified. The applicant must not ask another member of staff to show them the data or ask anyone else for a copy of the data. All communications must go through the DPL. A response will be provided promptly and in any event within one calendar month of receiving the request.

8.6 The UK General Data Protection Regulations and The Data Protection Act 2018 gives the DPL the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

8.7 All such requests must be referred to the DPL immediately and without undue delay.

8.8 If it is decided that a data subject access request is to be refused, the reasons will be fully documented in the DSAR Log and the data subject informed in writing, stating the reasons.

9. Complaints

9.1 It is recognised that some Data Subjects may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instance to the DPL - **dpl@wsc.ac.uk**.

Concerns or enquiries relating to the provisions of the UK General Data Protection Regulations and/or The Data Protection Act 2018 may be addressed to our DPO at The DPO Centre https://www.dpocentre.com/contact-us/. You also have the right to complain to the ICO about our operation of the system in relation to your personal data. The ICO can be contacted via their website at: https://ico.org.uk/global/contact-us/ or by telephone: **0303 123 1113.**

These rights do not alter the existing rights of anyone under any relevant grievance or disciplinary procedures.

10. Data breach

10.1 A data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

10.2 In the event that a data breach occurs, a thorough assessment of the breach will be made immediately by the DPL, as well as the DPO.

10.3 Immediate steps will be taken to ensure that the breach is contained, and the effects of the breach minimised and mitigated as much as possible.

10.4 If the data breach is deemed by the DPL to be reportable to the Information Commissioner's Office, the ICO will be notified within 72 hours of the discovery of the breach. The ICO can be informed via their website at: https://ico.org.uk/for-organisations/report-a-breach/ or by telephone: **0303 123 1113.**

10.5 In the case of a serious breach, Data Subjects whose data has been affected will be notified, in writing.

11. Compliance monitoring

11.1 The contact point for staff or members of the public wishing to enquire about the system will be the DPL by pre-arranged appointment - **dpl@wsc.ac.uk**

11.2 Upon request enquirers will be provided with:
- A copy of this policy
- An access request form if required or requested via FreeServe
- A subject access request form if required or requested
- A copy of the College's complaints procedures

11.3 All documented procedures will be kept under review and a report periodically made to senior management.

11.4 The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to senior management.

Revision History – Policy name

Revision date	Reason for revision	Section number	Changes made
Enter date	Enter reason	Enter section number	Enter details