CCTV Policy

1. Introduction

1.1 Chichester College Group (the Group) operates CCTV systems across all sites for the specific purpose of providing a safe and secure environment for our students, staff, visitors, the Group, and the property of all of those parties. Images are monitored and recorded.

1.2 Our CCTV systems capture images which include recognisable individuals which constitute personal data and are covered by the relevant Data Protection Regulations. This Policy should therefore be read in conjunction with the Group's Data Protection Policy. The images include personal appearance and behaviours. This information may be about students, staff, customers and clients, visitors and members of the public. The scope of monitoring includes individuals inside, entering or in the immediate vicinity of the area under surveillance.

1.3 Legislation requires the Group to ensure that personal data is protected to the best of our abilities and only used for the purposes it was collected. Failure to do so runs the risk of substantial fines, breach of the trust that data subjects put in us and significant adverse publicity.

1.4 Relevant legislation and codes of practice include:

- General Data Protection Regulations
- Data Protection Act 2018
- Protection of Freedoms Act 2012
- ICO Code of practice for surveillance cameras and personal information
- Surveillance Camera Commissioner's code of practice

2. Scope

2.1 This Policy applies to all CCTV systems planned or in use by the Chichester College Group.

2.2 Other policies are linked to this policy:

- The Document Retention Policy
- The Data Protection Policy
- The IT Security Policy

3. Purposes of the CCTV system

3.1 The specific purpose is to aid in the provision of a safe and secure environment for students, staff and visitors which expands to the following purposes:

- Providing a visual deterrent to those considering criminal acts
- Aiding in the detection and investigation of crime and disorder
- Complying with the terms of licensed premises

4. Operation of the system

4.1 The Director of IT and Director of Estates are responsible for the operation and maintenance of the CCTV systems on the various CCG College sites.

4.2 The system consists of cameras, digital recorders and monitoring stations in various locations around the sites.

4.3 There is signage, appendix A, distributed around the site to make individuals aware that there is CCTV monitoring taking place. This signage includes contact details of individuals with whom queries or complaints can be made.

4.4 Images will be recorded and retained in accordance with the Group Document Retention Policy. Integrity of the images will be maintained in a manner that protects the rights of the individual and retains the evidential value of the images should their use become necessary.

4.5 The operation of cameras will involve the following considerations:

- Cameras will not overlook adjacent private residences. Where this is unavoidable, the camera will be masked to prevent any invasion of privacy.
- Coverage will be primarily external to buildings and any internal requirements will be subject to further scrutiny and justification via a privacy impact assessment, appendix B.
- By the nature of a privacy impact assessment, this requirement will only be required where there is likely to be a risk to the rights and freedoms of data subjects, for example when significant changes are made to the

system.

4.6 The operation of digital recorders involves the following considerations:

- Digital recorders are sited in secure locations where only authorised members of staff have access.
- Network connected digital recorders are secured by complex passwords.

4.7 Access and monitoring of CCTV systems is limited to approved internal users with a legitimate business need to access them. An evaluation is made on a case-by-case basis and includes:

- Which cameras (or recorded images from which cameras) are required for the task.
- Whether the individual needs current view only or access to recorded images.
- Whether the reason for accessing the footage is consistent with the purposes for which the CCTV systems are operated.

4.8 Staff who have a need to request access to CCTV footage should complete an internal footage request form, appendix D, which will document the reason for accessing CCTV footage and enable the CCTV operator to locate the footage. This form does not need to be completed where footage is being requested as part of a right of access request, official police request or as part of another recognised disclosure method.

4.9 The Group does not endorse the use of covert surveillance.

4.10 No commercial use is or will be made of CCTV images.

4.11 There is no sound monitoring or recording by CCTV systems.

5. Body Worn Video Equipment

5.1 Body worn video (BWV) equipment consists of a small camera attached to a uniform which records visual and sound data.

5.2 The specific purpose of the recording is to safeguard staff, students and visitors during potentially violent and aggressive or anti-social behaviour incidents. The footage will also act as evidence for any subsequent investigations or prosecutions.

5.3 The use of BWV equipment is restricted to those internal users with a legitimate business need and prior approval. An evaluation is made on a case-by-case basis by the Group Director of IT or Deputy Chief Operating Officer and referred to GLT for approval.

5.4 BWV equipment should only be activated during an incident and continuous recording is strictly not permitted.

5.5 The operator should, where practicable, make a verbal announcement to indicate that the BWV equipment has been activated and verbally indicate recording will stop before ending the recording. Unless specific circumstances dictate otherwise, recording must continue uninterrupted from the moment it starts until the conclusion of the incident. These announcements should be captured on the recording.

5.6 Footage will be in an encrypted format while on the BWV equipment and transferred to secure storage without the need to remove the media. Footage will be securely stored.

5.7 Access to BWV footage is limited to those internal users with a legitimate business need to access them. An evaluation is made on a case-by-case basis.

6. Record keeping

6.1 Records are kept of accesses to the CCTV system and BWV archive and of any disclosures together with supporting documentation.

6.2 The Group have designed a form to record access to the CCTV system. A copy of the form can be found in appendix C.

7. Disclosures

7.1 Access to data by Data Subjects are provided via the procedure detailed in the Data Protection Policy recognising that it may be necessary to redact or deny requests to CCTV and BWV images where there is a possibility of disclosing data related to a third party.

7.2 Access to data via third parties will be denied except where it is in relation to the prevention or detection of crime, or the apprehension of offenders as per Schedule 2 part 1 paragraph 2 of the Data Protection Act.

7.3 Disclosures must be recorded in the right of access data protection register along with a copy of any supporting paperwork and details of any footage provided.

8. Complaints

8.1 Any complaints or concerns relating to the operation of the CCTV system must be made to the Data Protection Officer in writing:

email: dp@chichester.ac.uk
Address: Data Protection Officer
Chichester College Group
Westgate Fields
Chichester
PO19 1SB

9. Status of this policy

9.1 The policy was approved by the Group Leadership Team in TBC and supersedes all previous documentation and may be reviewed from time to time as necessary.

9.2 The operation of this policy will be kept under review by the Director of IT and Director of Estates.

9.3 It may be reviewed and varied from time to time by the Group Leadership Team.

Date approved:	22 October 2020
Approved by:	Group Leadership Team
Date reviewed:	October 2020
Date of next review:	October 2022

Appendix A – Example CCTV signage

CCTV in operation

Images are being recorded for the purpose of crime prevention and public safety

CCTV system is operated by Chichester College Group

For information contact:
dp@chichester.ac.uk

Appendix B – DPIA for internal CCTV

Date of assessment:	
Review date:	
Name of person making assessment:	
Data Protection Officer:	

Location of camera system being assessed:

Campus	Building/Area	Camera type
e.g. Chichester	e.g. Premier Shop	e.g. 2 x static

What are the problems that you need to address in defining your purpose or using the surveillance camera system?

Can surveillance software technology realistically mitigate the risks attached to those problems?

What other less privacy-intrusive solutions such as improved lighting have been considered?

What are the views of those who will be under surveillance?

What are the benefits to be gained from using surveillance cameras over alternative solutions?

Have any data protection by design and default features been adopted to reduce privacy intrusion?

How will people be informed that they are under surveillance? For example is there the need for additional signage?

Is the camera system/hardware/software/firmware being considered compatible with existing systems and how do you know the desired benefits will be delivered now and in the future?

Approved by:

Name:	
Date:	
Comments:	

DPO advice:

Name:	
Date:	
Comments:	

DPO comments accepted or approved by:

Name:	
Date:	
Comments:	

Appendix C - CCTV Access Log

CCG CCTV Access Log

Ref #	Date	Person	Reason	Footage viewed and notes (DVRs, Cameras, Times/Dates)	Successful?	S29	SAR	Saved?	Taken?

Appendix D – Internal Footage Request Form

This form should be completed by CCG staff who would like access to CCTV footage captured by the Group's CCTV system as part of an internal investigation. Completion of the form does not guarantee access to footage will be granted, however will be used to document the business case for accessing footage and to enable the CCTV operator to locate the relevant footage.

This form does not need to be completed if CCTV footage is being requested as part of a right of access request or if a request has been received by an official authority or law enforcement agency. These requests should be handled under the Group Data Protection Policy by the Data Protection Officer.

Date & Time of Incident:	
Details of Incident:	
Staff Signature:	
Print Name of Staff Member:	
CCTV Log Number:	
Date & Time of removal of images:	
Name of CCTV Operator:	
Name(s) of person(s) viewing images:	
The reason for viewing:	
The outcome, if any of the viewing:	

Please return completed forms to the College Community Support Officer (CCSO) on your campus or to the Data Protection Officer: dp@chichester.ac.uk.