Board of Management

People & Culture Committee

Date of Meeting	**Wednesday 15 May 2024**
Paper No.	**PCC3-D**
Agenda Item	**4.4**
Subject of Paper	**CCTV Code of Practice & EQIA**
FOISA Status	**Disclosable**
Primary Contact	**John Gribben**
Date of production	**3 May 2024**
Action	**For Approval**

1. Recommendations

The CCTV Code of Practice has been reviewed and is ready for the People & Culture Committee approval. An Equality Impact Assessment has been carried out and included in this paper. Once approved the CCTV Code of Practice will be published on MyConnect for all staff.

2. Purpose

The purpose of this paper is to provide a copy of the reviewed CCTV Code of Practice and Equality Impact Assessment (EQIA), to the People and Culture Committee and to request their approval.

The purpose of this CCTV Code of Practice is to ensure that the operation of the CCTV system is consistent with the legal obligations of the College as a Data Controller under data protection law.

3. Consultation

The CCTV Code of Practice has been reviewed by the Associate Director, People & Culture (Health & Safety) through consultation with the Front of House Manager, and the Front of House Co-ordinator. The Data Protection Officer provided legal guidance and the IT Technical Manager (Infrastructure) provided technical guidance on secure sharing of CCTV footage. The EDI Manager, Head of Student Support & Wellbeing and the Learning Support manager, were all consulted with during the EQIA assessment.

4. Key Insights

4.1 The CCTV Code of Practice was last reviewed in November 2018. Since then, there have been changes to roles and responsibilities, which have been amended to reflect our current structure.

4.2 There was a requirement to tighten up the process for retaining images and find a more secure process for sharing footage with external organisations.

4.3 The Data Protection Officer provided a thorough review of the Code of Practice and provided more detailed information on the legal requirements.

4.4 The Data Protection Officer added additional information on Data Subject Requests which was missing from the previous version.

4.5 A table has been added to allow College staff to determine if it they are able to comply with a request to view CCTV footage and to understand the legal basis they are relying on under the UK GDPR when complying with a request.

4.6 Front of House staff are all trained on GDPR and on putting the CCTV Code of Practice into effect. Training is recorded on their personal file.

4.7 A digital form has been developed to be used when CCTV footage is being requested by staff for investigative purposes and approval is recorded on this digital form.

5. Impact and Implications

The use of CCTV surveillance must be consistent with respect for individuals' privacy and the purpose of this Code of Practice is to ensure that the operation of the CCTV system is consistent with the legal obligations of the College as a Data Controller under data protection law; the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (as amended by the EU Exit Regulations) and all and any laws and regulations that may be applicable to the UK in the future ('Data Protection Legislation').

The use of CCTV by the College is necessary and proportionate, and this CCTV Code of Practice demonstrates that the use of CCTV and associated processing of personal data by the College, aligns with the principles of Data Protection Legislation. What this means in practice is that the College is transparent about its use of CCTV and has a clear purpose to use it. There is a strategy to minimise processing, maintain appropriate security controls, restrict access and a short retention period applies to mitigate the risk of excessive processing. There is an established process in place to ensure that CCTV is only shared in limited circumstances, when the law permits.

Appendices

Appendix 1 - CCTV Code of Practice V3

Appendix 2 - CCTV Code of Practice Equality Impact Assessment

Appendix 1

CCTV Code of Practice

© 2024 City of Glasgow College

Charity Number: SCO 36198

DRAFT

Contents

1. PURPOSE

This document should be read in conjunction with the College's Data Protection Policy and Request for Personal Data Procedure to give the fullest picture of the College's data protection privacy compliance framework. The use of CCTV surveillance must be consistent with respect for individuals' privacy and the purpose of this Code of Practice is to ensure that the operation of the CCTV system is consistent with the legal obligations of the College as a Data Controller under data protection law; the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (as amended by the EU Exit Regulations) and all and any laws and regulations that may be applicable to the UK in the future ('Data Protection Legislation').

The use of CCTV by the College is necessary and proportionate, and this CCTV Code of Practice demonstrates that the use of CCTV and associated processing of personal data by the College, aligns with the principles of Data Protection Legislation. What this means in practice is that the College is transparent about its use of CCTV and has a clear purpose to use it. There is a strategy to minimise processing, maintain appropriate security controls, restrict access and a short retention period applies to mitigate the risk of excessive processing. There is an established process in place to ensure that CCTV is only shared in limited circumstances, when the law permits.

The CCTV system will only be used to respond to the following key objectives:

- To detect, prevent or reduce the incidence of crime
- To prevent and respond effectively to all forms of harassment and disorder.
- To reduce the fear of crime
- To create a safer environment
- To gather evidence fairly and transparently
- To provide emergency services assistance
- To assist with health and safety and other serious occurrences

2. SCOPE

For the purpose of this Code of Practice CCTV equipment includes cameras, transmission, monitoring and retrieval equipment as defined in the BS 7958 – CCTV, Management and Operation Code of Practice.

There are cameras located in publicly accessible space both inside and outside of the College's buildings including the Halls of Residence, monitoring both public and secure areas. Areas covered include hallways, lift lobbies, communal eating and seating areas. Most of these cameras are static, although there are fully functional cameras in strategic locations including in carparks, stairways, foyers and libraries.

The external cameras cover the area around the College buildings, the car park areas and approaches to the campus. Internal cameras generally cover transit spaces such as corridors, canteen and reception areas.

In line with the data protection principle of data minimisation, all CCTV cameras are configured to record images only; any sound recording facilities are switched off or disabled. Neither facial recognition nor gait recognition are utilised by City of Glasgow College.

The public and College community will be made aware of the presence of the CCTV by clearly visible and legible signage, that state that CCTV is in operation, identifies the College as the Data Controller, provides contact details for the College and, as far as possible, sets out the purposes for processing the CCTV images.

To ensure privacy, wherever practicable, the College CCTV cameras are prevented from focusing directly or dwelling on private residences or other office spaces. Where it is not practicable to prevent the cameras from capturing images of such areas electronic privacy masks are installed on these cameras. Where cameras do not have this functionality, they will be replaced. Appropriate training will be given to system operators to ensure that they are made aware that they should not be monitoring such areas and to actively do so is a breach of data protection legislation and a disciplinary and a criminal offence.

The CCTV equipment and location of each camera will be chosen to meet the quality and

image capture standards necessary to achieve the College's purposes for processing the images. The location and technical specification of each camera will take account of the field of vision of the camera, light levels and other environmental conditions and minimise the capture of images that are not relevant to the purposes for which the College use CCTV.

The suitability and functionality of the CCTV cameras for the College's purpose will be kept under review and equipment updated or replaced where appropriate.

Cameras are controlled and monitored at Level 0 Security Control rooms at City and Riverside Campuses. There are a smaller number of cameras in the halls of residence, which are controlled centrally at City and monitored at the halls of residence.

This Code of Practice only applies to all CCTV equipment operated by City of Glasgow College.

3. RESPONSIBILITIES

Associate Director People & Culture (H&S): Accountable for the college's CCTV system and for ensuring appropriate and up to date procedures are in place and for compliance with all relevant legislation and regulatory guidance. Authority to allow lawful access to College CCTV systems and footage.

Front of House Manager: Responsible for the operation of the college CCTV equipment and for ensuring that no unauthorised or inappropriate use is made of the system. Responsible for ensuring procedures are followed and for compliance with all relevant legislation and regulatory guidance. Responsible for ensuring quarterly audits of the system are carried out.

Front of House Co-ordinator: Responsible for the operation of the college CCTV equipment and for ensuring that no unauthorised or inappropriate use is made of the system. Responsible for carrying out quarterly audits of the system.

Front of House Officer: Responsible for monitoring CCTV installation including

playback of images.

Head of Student Accommodation and Services: Responsible for ensuring compliance with this Code in the College's Halls of Residence.

Data Protection Officer: Responsible for advising the organisation on their obligations in relation to data protection legislation.

4. OPERATIONS

Control Room Operation

The system shall be operated and maintained in accordance with this Code of Practice. A paper copy of this Code of Practice is located at the CCTV control desk at both Campuses and in the halls of residence for reference purposes. An electronic copy of the most up-to-date version of the Code will be maintained on MyConnect and on the College's website. All operating staff must comply with the guidelines and operating instructions for the CCTV control equipment.

4.1 Access to Control Room

Access to the control rooms is limited only to those who have a clear operational reason and the appropriate authority to gain access, including cleaning staff or engineers effecting repairs. The Associate Director People & Culture (H&S) is responsible for permitting lawful access to the control rooms and College CCTV systems and footage. All requests to access the Control Room must be submitted to the Data Protection Officer prior to access being extended. All persons visiting the control room with the purpose of viewing recorded data will be required to sign the CCTV log. All staff working in the Control Room and monitoring CCTV cameras will be made aware of the sensitivity of handling CCTV images and recordings and will be provided with appropriate training. Any misuse of information obtained from a recording will be considered a serious disciplinary offence and may be reported to the Police.

4.2 Authorised Operation of CCTV Equipment

CCTV equipment may only be used for the defined purposes as set out in the introduction

to this code. Any person who uses or requires another to use the system for purposes not within the defined scope of the code will be committing a breach of the college's disciplinary procedures, a breach of data protection legislation and may be committing a criminal offence. Only persons who have received full training on the operation and use of the CCTV equipment should be authorised to operate the equipment.

Suspicious activities or incidents monitored and recorded by CCTV equipment must be logged by the operator in the CCTV viewing log. The date, time, location, camera number and type of incident are to be noted for possible investigation.

All staff who operate CCTV require to undergo a programme of training on the system operation, and data protection. Documented training records for each authorised CCTV operator shall be maintained by the Front of House Co-ordinator.

4.3 Liaison with the Police

Suspicious activities or incidents which may be criminal in nature must be brought to the attention of Police as soon as possible. A log of the incident number should be recorded.

4.4 Retention of Images

Data protection law means that personal data must not be retained for longer than is necessary for the purpose for which it was collected. College CCTV data is kept for 30 days, after which time the data is destroyed.

The DVR (Digital Video Recorder) units are programmed to automatically delete any recorded video files which are older than 30 days. This data is stored locally on the system and is password protected with only authorised users having access. Data can be transferred electronically using a digitally secure file format and password protected. Password must be sent separately to the file. The use of USB is discouraged and should only be used when there is no other alternative (often the Police will request footage via USB) in this case file should be password protected and the location of the USB logged on the CCTV log.

Any images retained (electronically or on USB Memory device) to be used as evidence are kept securely within the Front of House SharePoint (and password protected) or in the case of USB, securely in the Control Room. The Front of House Officer or Front of House Manager is responsible for production of any images to be retained for evidential purposes. Any such images will be retained only for as long as required (for the purpose of providing evidence) and will then be destroyed.

Access to the DVRs is limited to access at the DVR units themselves or authorised workstations, and only then to persons who have correct levels of access. The DVRs are all only accessible to persons with correct login identification and password. The DVRs and their associated monitors are all located in rooms away from the general public where private viewing e.g. by the Police, can be supervised and facilitated.

4.5 Recording of Images

It is very important that any risks to an individual's privacy are considered, and appropriate steps are taken to prevent unauthorised access to recordings. It is a disciplinary, a breach of data protection legislation and criminal offence to make or take any recordings from the CCTV digital recording systems without proper authority in terms of this Code of Practice.

Where digital video evidence is to be used by the Police or other law enforcement authority an entry will be made into CCTV viewing log, which details what has been recorded and when this was done. It will also record the person who carried out the recording and the police officer whom the recording was given to. When a recording of images from the DVR is made, the location of all copies of the file are to be noted in the CCTV viewing log, the location of all copies of recording must be constantly known and recorded.

The USB Memory device which is handed to the Police will be marked, in permanent marker pen, to help tracking of the recording. The detail of all copies of footage recorded from the CCTV system onto USB Memory device are to be recorded in the CCTV viewing log. Each USB Memory device is to be given an individual number and recorded in the CCTV viewing log.

4.6 Viewing of Recorded Images

Only authorised persons will be permitted to view recorded images upon submitting a valid request, in writing. This may include an officer from an authorised law enforcement agency, such as the police. The College will only share these images where there is a legal basis for doing so, for example in the detection and prevention of crime. The viewing of recorded images is only to be carried out in connection with the purposes defined in section 2 and in compliance with Data Protection legislation. Any use outside the defined purposes is a breach of the Data Protection legislation.

Recorded images must only be viewed in a secure area where the images cannot be overlooked by unauthorized persons. Each time a DVR is accessed a password must be entered. The reviewing of recorded images is documented on the CCTV viewing log.

4.7 Removal of Images

Removal or extraction of any recorded images from the Colleges control requires to be authorised by the Associate Director, People & Culture (H&S) or the Data Protection Officer and clearly recorded in the CCTV viewing log. CCTV images or footage must never be uploaded onto social media networks.

4.8 Care of Digital Recording Systems

Digital video recorders and cameras are maintained by Glasgow Learning Quarter (GLQ) as part of their programme of routine maintenance. GLQ must complete the CCTV access log when undertaking repairs or maintenance of the systems. All digital video recorders are connected to a secure server on the Colleges network and are not available to persons outside the College. All Digital Video Recorders must be held within a secure place and must be password protected to prevent unauthorised access to the system, software or recordings.

5. DATA PROTECTION

Personal data includes any image from which an individual may be identified. The processing of personal data includes the recording, viewing, storage and destruction of personal data. The College is responsible for all CCTV owned and operated by the College and is the data controller as defined by data protection law.

5.1 Access to CCTV data

All requests to view CCTV footage will be dealt with in accordance with data protection law and the College's Requests for Personal Data Procedures and will be communicated to the Associate Director, People & Culture (H&S) or the Data Protection Officer. Disclosure of recorded images to third parties will be controlled and consistent with the purpose for which the system was established. Any requests for images and details of subsequent disclosures by police, should be recorded and a record kept by Security Team.

Requests from the Police

Requests for information by the Police and other authorities must be accompanied by the relevant Police Scotland Data Protection form duly signed and countersigned by the relevant police officers. The form should state clearly what information is requested, the purpose of obtaining the information i.e. required for an investigation concerning the apprehension or prosecution of offenders.

Disclosures in relation to the prevention or detection of crime and the apprehension or prosecution of offenders generally occur, for obvious reasons, without the consent of the individual whose personal data is being disclosed. This is lawful and is covered by an exemption in terms of data protection law.

The legal basis the College relies on for the processing of personal data is performance of a task carried out in the public interest under Art.6(1)(e) of the UK GDPR. Where the data being processed by the College falls within the scope of special category data, the legal basis for processing will be one of the following:

(a) processing is necessary for the establishment, exercise or defence of legal claims under Art 9(2)(f) of the UK GDPR; or

(b) processing is necessary for a task carried out in the public interest under Art 9(2)(g) of the UK GDPR.

It is at the College's discretion to disclose the data to the Police, unless there is an overriding legal obligation (for example a court order) where we have no discretion.

However, where College staff have contacted the police to report a crime then a request form need not be completed by the Police since the College has initiated the disclosure and is entitled to share the data with the police for the prevention and detection of crime. A record of the police incident and report must be made in the CCTV log.

Internal requests from staff to view footage

Any internal requests submitted by college staff to view CCTV, for instance in relation to a disciplinary investigation, must be escalated to the Associate Director People & Culture (H&S) or the Data Protection Officer immediately for consideration, who will review the request.

CCTV system operating staff must receive sufficient training on how to manage and escalate any internal requests for access to the system to reduce the likelihood of unfair use.

The request must clearly set out why the request is being made and how it might assist the relevant matter. Access should be given only in exceptional circumstances e.g., where the evidence provided by a CCTV image is the best evidence available and is, in the view of the Associate Director People & Culture (H&S), essential to ensuring a fair hearing for a student or member of staff.

All students and staff are entitled to seek access to their images using the subject access request procedures set out below in Section 5.2.

Emergency access to CCTV systems

Footage or live data may be accessed without authorisation in emergency situations where it is vital that the footage is made available immediately e.g., where there is a very serious medical emergency. The fact that access was given must still be detailed in the CCTV log and details taken e.g. Police incident number, details of police attending etc.

Where the request is considered to be an emergency and time is of the essence the member of staff, with line management authority where reasonably possible, will judge whether or not to provide the information without the submission of an appropriate form. Providing access to images to the Police without a completed standard form should be considered to be exceptional and not standard practice and is at the College's discretion unless overruled by legal obligation, for example a search warrant. Advice should be sought from the Data Protection Officer before disclosing images without a completed police request form.

Other law enforcement agencies

Other law enforcement agencies may request for personal data. Any request must:

- Be clearly identifiable as from the agency in question i.e. in writing, on headed paper, and signed by an officer of the agency. The College should take any steps it deems necessary to ensure as far as is practicable that the request is legitimate and that the requestor's identity is verified.
- Describe the nature of the information which is required.
- Describe the nature of the investigation (e.g. citing any relevant statutory authority to obtain the information).
- Certify that the information is necessary for the investigation.

Each request will be assessed on a case-by-case basis. In most cases the decision as to whether the College should provide CCTV footage will be taken by the Associate Director People & Culture (H&S) (or their depute). Each request should be communicated to the Data Protection Officer prior to the disclosure of the images. If there is any doubt as to whether information should be released then the Data Protection Officer must be consulted for advice.

Any unauthorised disclosure or misuse of CCTV data by staff is a serious matter and may be considered a disciplinary matter or even a criminal offence.

5.2 Data Subject Access Requests (DSAR)

Requests from individuals to view footage of themselves should be treated as requests

for personal data and follow the College's Requests for Personal Data Procedures. Where a potential data subject wishes to obtain access to/copies of the recorded CCTV images they may put the request in writing, but are not obliged to do so. The College has 30 calendar days to respond to a DSAR, therefore they must be immediately referred to the Data Protection Officer.

The Data Protection Officer will process any DSAR requesting CCTV footage in conjunction with Associate Director People & Culture (H&S). Where third parties can be identified from the footage their images will have to be obscured to prevent such identification. If images of third parties cannot be suitably obscured the College may request consent from the relevant third parties, to share the data. Where is it not practically possible to do so, the College may not be able to grant the data subject access to the data. The Data Protection Officer will provide advice to ensure compliance with the law. Where possible, the data should be provided to the data subject in a format designated by the data subject.

5.3 Data Subject Requests

Under data protection legislation, data subjects have additional rights including; the right to erasure, to rectification, to object to processing, to restrict processing and to data portability. Requests to exercise other rights under data protection legislation such as the right to correction or erasure of personal data should be dealt with in terms of the College's Requests for Personal Data Procedures and referred immediately to the Data Protection Officer.

The right to rectification does not apply. In terms of the right to erasure, data subjects must be informed that CCTV footage is deleted following a period of 30 days so no erasure request may be required. Where an investigation is ongoing, the request may be refused by the College. The rights to object and to restrict processing may be practically impossible to comply with in this instance, and this must be clearly explained to the data subject. The right to data portability means that the data subject wishes to receive a copy of their data in order to share with a third party. Where it is practically possible, this request should be complied with.

5.4 Legal Basis

The purpose of the below table is to allow College staff to determine if it they are able to comply with the request and to understand the legal basis they are relying on under the UK GDPR when complying with a request.

Purpose	Requestor	Legal Basis	Description
Monitoring of CoGC premises	CCTV Operatives	Public interest and public task.	CCTV Operatives must be appropriately trained and abide with the CCTV Policy and Data Protection Policy.
Crime prevention	Law enforcement	Public interest, public task and legal claims	Viewing and sharing of footage must be authorised by the Associate Director People & Culture (H&S) or the Front of House Officer and clearly recorded in the CCTV viewing log.
Repairs and maintenance	GLQ	Public interest	GLQ must complete the CCTV access log.
Disciplinary Hearings	CoGC staff above a certain grade	Employment contract	Footage may be used in the course of disciplinary procedures.
Subject Access Requests	Individuals; students and staff	Consent	Individuals may view their own data. Measures must be taken to safeguard the privacy of other individuals in the footage. CCTV footage may be viewed by CoGC Front of House staff to comply with subject access requests where appropriate.
Erasure requests	Individuals; students and staff	Consent	CCTV footage may be viewed by CoGC Front of House Staff to comply with erasure requests where appropriate. Where an investigation is ongoing, this request may be refused.
Right to object, restrict processing	Not applicable	Not applicable	Not applicable
Right to rectification	Not applicable	Not applicable	Not applicable

Right to data portability	Individuals; students and staff	Not applicable	Where possible (where the data has been collected within 30 days of the request or where there is an investigation ongoing) the data subject should be provided with a copy of their data.

6. COMPLIANCE

The College will at all times comply with current UK Data Protection Legislation. This Procedure takes into consideration the recommendations set out in the UK ICO CCTV Code of Practice.

All staff dealing with CCTV equipment and recordings should be aware of the College's Data Protection Policy and Procedures. In addition, these staff members should receive regular and appropriate training to ensure they are aware of the correct operation of the system and handling of personal data.

Any misuse of information obtained from a video recording is a breach of Data Protection Legislation. Any such breach is a serious issue and may result in disciplinary action being taken against the member of staff involved. In certain circumstances individual members of staff may also be referred to the police if it appears that an offence has been committed e.g. personal data has been illegally and intentionally misused for personal gain and not in the College's interest.

7. FURTHER HELP AND ADVICE

For further advice and assistance contact:

Data Protection Officer: dpo@cityofglasgowcollege.ac.uk

8. POLICY REVIEW

This policy will be subject to regular review and audits to ensure ongoing compliance with data protection legislation. The necessity and proportionality of the use of CCTV must be regularly reviewed and justified any changes in the procedures or utilisation of CCTV must be documented in this policy.

9. DOCUMENT CONTROL REVIEW

Approval Status		
Approved by	**SMT**	
Date Approved		
EQIA Status	EQIA Conducted?	
Proposed Review Date	2 years	
Lead Department	People & Culture – Front of House Services	
Lead Officer(s)	John Gribben & Jill Loftus	
Board Committee	Not relevant	

10. DEFINITIONS

Data Protection Officer: the officer with oversight of organisational and technical measures and controls to comply with the Data Protection Act.

Personal Data: data which relates to a living person who can be identified from the data and other information that the Data Controller holds or is likely to receive.

Subject Access Request: A request, whether written or oral, formal or informal, for a copy of one's own personal data.

Data subject: the owner of the personal data under consideration.

11. REVISION LOG

Version Date	Section	Description
Version 2 13.11.2018	1	Purpose - additional line added to reflect amendments by the EU Exit Regulations
	2	Scope – additional detail added "Neither facial recognition nor gait recognition are utilised by City of Glasgow College.
	3	Responsibilities – amended to reflect structure change – • Amended from Head of Estates to Associate Director People & Culture (H&S) • Front of House Manager added with associated responsibilities. • Amended from Building Services Manager to Front of House Co-ordinator • Role of Security Officer & Concierge amended to Front of House Officer • Director of Corporate Support responsibility replaced by DPO • Data Protection Officer: Changed to reflect DPO comment - The DPO is not directly responsible for the organisation's compliance, but rather to advise the organisation on how they can comply - updated definition accordingly.

	4.1	Access to Control Room – slight change in wording without change to meaning. Amended access to CCTV "footage" to "Control room" • Amended from Head of Estates to Associate Director People & Culture (H&S)
	4.4	Retention of images • Additional detail provided on the secure transfer of data • CDROM or DVD removed and replaced with - Data can be transferred electronically using a digitally secure file format and password protected. Password must be sent separately to the file. The use of USB is discouraged and should only be used when there is no other alternative, in this case file should be password protected and the location of the USB logged on the CCTV log. • Production of images amended from Building Services Manager to Front of House Co-ordinator
	4.5	Recording of Images • USB Memory device replaces CDROM or DVD
	4.6	Viewing of Recorded Images • Permitted only with a valid request, in writing added
	4.7	Removal of Images • amended from Building Services Manager to Senior Security & Senior Concierge • Authorisation by the DPO added • Added - CCTV images or footage must never be uploaded onto social media networks
	5.1	Access to CCTV data • Front of House replaces Building service • Director of Corporate Support responsibility replaced by Associate Director People & Culture (H&S) • Added - Advice should be sought from the Data Protection Officer before disclosing images without a completed police request form. • Other law enforcement agencies – further detail added to the process to follow in line with DPO guidelines • Added - Any unauthorised disclosure or misuse of CCTV data by staff is a serious matter and may be considered a disciplinary matter or even a criminal offence.
	5.2	Title amended from SAR to Data Subject Access Requests (DSAR) • Responsibility for processing any DSAR requests moved from The Director of Corporate Support to the DPO • Added - The Data Protection Officer will provide advice to ensure compliance with the law.

		• Added - Where possible, the data should be provided to the data subject in a format designated by the data subject. • Requests to exercise other rights under data protection removed and replaced by more detail in 5.3
	5.3	Data Subject Requests – new section added by DPO giving more detail on: • Under data protection legislation, data subjects have additional rights • The right to rectification does not apply • The rights to object and to restrict processing may be practically impossible to comply with • The right to data portability
	7	Further help & advice • AD name removed • Change of DPO contact to DPO email address
	8	Policy review statement added
	9, 10, 11	Altered titles to reflect adding section 8 • Revision log updated with all revisions from 2018 V2

CITY OF GLASGOW COLLEGE

Equality Impact Assessment (EqIA) Revised Form 2019

The Public Sector Equality Duty (PSED) and protected characteristics are detailed at the end of this form.
Refer to the EqIA Guidance Document for more Information on how to complete this form.

Title of Policy, Procedure, or Relevant Practice:	CCTV Code of Practice	**Lead Officer:**	Jill Loftus
Type of Policy, Procedure, or Relevant Practice:	New: ☐ Existing/Reviewed/Revised: ◯	**Date of Assessment:**	11/04/2024

Step 1: Outcomes and Potential Impacts

What are the intended consequences (outcomes) of the policy, procedure or practice?

The CCTV Code of Practice ensures the use of CCTV surveillance is consistent with respect for individuals' privacy and the purpose of the Code of Practice is to ensure that the operation of the CCTV system is consistent with the legal obligations of the College as a Data Controller under data protection law; the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (as amended by the EU Exit Regulations) and all and any laws and regulations that may be applicable to the UK in the future ('Data Protection Legislation').

The use of CCTV by the College is necessary and proportionate, and this CCTV Code of Practice demonstrates that the use of CCTV and associated processing of personal data by the College, aligns with the principles of Data Protection Legislation. What this means in practice is that the College is transparent about its use of CCTV and has a clear purpose to use it. There is a strategy to minimise processing, maintain appropriate security controls, restrict access and a short retention period applies to mitigate the risk of excessive processing. There is an established process in place to ensure that CCTV is only shared in limited circumstances, when the law permits.

The CCTV Code of Practice explains to staff that the system will only be used to respond to the following key objectives:

To detect, prevent or reduce the incidence of crime
To prevent and respond effectively to all forms of harassment and disorder.
To reduce the fear of crime
To create a safer environment
To gather evidence fairly and transparently
To provide emergency services assistance
To assist with health and safety and other serious occurrences

Step 2: Consideration of Evidence and Information

2A. What information do you plan to use as the basis of this EQIA?
(What information is available and if information is lacking, how will you address this shortfall?)

The CCTV Code of Practice 2024
The College's Data Protection Policy
Request for Personal Data Procedure

2B. Please indicate potential positive, neutral and negative impacts in relation to each protected characteristic.

(What does the information indicate about potential **positive, neutral and negative** impacts on people who share protected characteristics? Are the needs of people with different characteristics met? Does the policy, procedure, or practice affect some groups differently?)

Protected Characteristic	**Check the relevant box and provide an explanation for each option chosen, with reference to evidence, or information. Note: in some cases, impacts can be both positive and negative.**		
Age	Positive ☑ 1. Enhanced safety: CCTV cameras can provide a sense of security, especially in areas with high foot traffic or during late hours. 2. Prevention of bullying: CCTV surveillance may deter bullying behavior, as the presence of cameras can make perpetrators think twice before engaging in such acts. 3. Assistance in emergencies: CCTV footage can aid in quickly responding to emergencies, such as accidents or medical incidents. 4. Enhanced security: CCTV cameras can provide a sense of security particularly in areas with historical incidents of theft or vandalism.	Neutral ☐	Negative ☑ 1. Privacy concerns: Students/staff may feel that their privacy is being invaded by CCTV surveillance. 2. Stigmatization: The presence of CCTV cameras may make students/staff feel like they are under constant scrutiny or suspicion, leading to feelings of discomfort or anxiety. 3. Fear of punishment: Students may worry that minor infractions or mistakes caught on CCTV cameras could result in disciplinary action, creating a culture of fear rather than one of trust and support. 4. Perceived age discrimination: Students/Staff may feel targeted or unfairly treated by the presence of CCTV cameras, especially if they perceive surveillance as singling them out based on their age.

2B. cont'd - Please indicate potential positive, neutral and negative impacts in relation to each protected characteristic.			
Protected Characteristic	**Check the relevant box and provide an explanation for each option chosen, with reference to evidence, or information. Note: in some cases, impacts can be both positive and negative.**		
Disability	Positive ☑ 1. Enhanced safety: CCTV can provide an added layer of security for students/staff with disabilities, particularly those who may be more vulnerable to harassment or bullying. 2. Assistance in emergencies: CCTV footage can aid Front of House Officers in responding quickly to emergencies, including medical incidents or instances where a student with disabilities requires assistance. 3. Deterrence of crime: The presence of CCTV cameras may deter criminal activity on campus, creating a safer environment for all students, including those with disabilities.	Neutral ☐	Negative ☑ 1. Privacy concerns: Students/staff with disabilities may have concerns about their privacy being compromised by CCTV surveillance. 2. Stigmatization: Some students/staff with disabilities may feel stigmatized or singled out by the presence of CCTV cameras, particularly if they perceive the surveillance as targeting them specifically. 3. Communication barriers: Front of House staff with disabilities who rely on assistive technologies or communication aids may face challenges in accessing CCTV footage if the systems are not designed with accessibility in mind.
Gender Reassignment	Positive ☑ 1. Enhanced safety: CCTV cameras can contribute to a safer environment for transgender students/staff by deterring harassment, bullying, and discrimination. 2. Documentation of incidents: CCTV footage can provide evidence in cases of discrimination or violence against transgender individuals, helping to hold perpetrators accountable and ensure justice.	Neutral ☐	Negative ☑ 1. Privacy concerns: Transgender individuals may have concerns about their privacy being violated by CCTV surveillance. 2.Targeted surveillance: Transgender individuals may feel targeted or singled out by the presence of CCTV cameras, particularly if they perceive the surveillance as monitoring their behavior or gender presentation. 3. Misgendering: If Front of House personnel or others reviewing CCTV footage misgender transgender individuals based on their appearance or presentation, it can lead to feelings of distress, invalidation, and further marginalization. 4. Fear of outing: Transgender students/staff may fear being inadvertently outed if they are visibly transgender in CCTV footage that is reviewed by others without their consent, potentially exposing them to discrimination or harassment.

2B. cont'd - Please indicate potential positive, neutral and negative impacts in relation to each protected characteristic.			
Protected Characteristic	**Check the relevant box and provide an explanation for each option chosen, with reference to evidence, or information. Note: in some cases, impacts can be both positive and negative.**		
Marriage & Civil Partnership	Positive ☑ 1. Enhanced safety: CCTV cameras can contribute to a safer environment for students/staff by deterring incidents of harassment, bullying, or violence. 2. Assistance in emergencies: CCTV footage can aid Front of House staff in responding quickly to medical emergencies or incidents where a student/member of staff requires assistance. 3. Documentation of incidents: CCTV footage can provide evidence in cases of discrimination or mistreatment helping to ensure accountability and protection of their rights.	Neutral ☐	Negative ☑ 1. Privacy concerns: Students/staff may have concerns about their privacy being compromised by CCTV. 2. Increased stress: CCTV surveillance can contribute to feelings of stress or anxiety among students/staff, especially if they feel like their every move is being monitored or scrutinized.
Pregnancy & Maternity	Positive ☑ 1. Enhanced safety: CCTV cameras can contribute to a safer environment for pregnant students/staff by deterring incidents of harassment, bullying, or violence. 2. Assistance in emergencies: CCTV footage can aid Front of House staff in responding quickly to medical emergencies or incidents where a pregnant student requires assistance. 3. Documentation of incidents: CCTV footage can provide evidence in cases of discrimination or mistreatment of pregnant students/staff, helping to ensure accountability and protection of their rights.	Neutral ☐	Negative ☑ 1. Privacy concerns: Pregnant students/staff may have concerns about their privacy being compromised by CCTV. 2. Increased stress: CCTV surveillance can contribute to feelings of stress or anxiety among pregnant students/staff, especially if they feel like their every move is being monitored or scrutinized.

2B. cont'd - Please indicate potential positive, neutral and negative impacts in relation to each protected characteristic.

Protected Characteristic	Check the relevant box and provide an explanation for each option chosen, with reference to evidence, or information. Note: in some cases, impacts can be both positive and negative.		
Race	Positive ☑ 1. Enhanced safety: CCTV cameras can provide a sense of security 2. Prevention of bullying: CCTV surveillance may deter bullying behavior, as the presence of cameras can make perpetrators think twice before engaging in such acts. 3. Assistance in emergencies: CCTV footage can aid in quickly responding to emergencies, such as accidents or medical incidents. 4. Enhanced security: CCTV cameras can provide a sense of security particularly in areas with historical incidents.	Neutral ☐	Negative ☑ 1. Privacy concerns: students/staff may have concerns about their privacy being compromised by CCTV surveillance, especially in areas such as areas where they may seek privacy or confidentiality. 2. Targeted surveillance: Students/staff may feel targeted or singled out by the presence of CCTV cameras, particularly if they wrongly perceive the surveillance as monitoring their behavior or cultural activities based on their ethnicity or background. 3. Fear of discrimination: Students/staff may fear being unfairly targeted or scrutinized by Front of House staff based on stereotypes or biases, leading to feelings of distrust or discomfort. 4. Misinterpretation of cultural behaviors: Front of House staff or others reviewing CCTV footage may misinterpret cultural behaviors or interactions among students/staff, potentially leading to misunderstandings or unwarranted interventions.
Religion or Belief	Positive ☑ 1. Enhanced safety: CCTV cameras can provide a sense of security 2. Prevention of bullying: CCTV surveillance may deter bullying behavior, as the presence of cameras can make perpetrators think twice before engaging in such acts. 3. Assistance in emergencies: CCTV footage can aid in quickly responding to emergencies, such as accidents or medical incidents. 4. Enhanced security: CCTV cameras can provide a sense of security particularly in areas with historical incidents.	Neutral ☐	Negative ☑ 1. Privacy concerns: students/staff may have concerns about their privacy being compromised by CCTV surveillance, especially in areas such as areas where they may seek privacy or confidentiality. 2. Targeted surveillance: Students/staff may feel targeted or singled out by the presence of CCTV cameras, particularly if they wrongly perceive the surveillance as monitoring their behavior or cultural activities based on their ethnicity or background. 3. Fear of discrimination: Students/staff may fear being unfairly targeted or scrutinized by Front of House staff based on stereotypes or biases, leading to feelings of distrust or discomfort. 4. Misinterpretation of behaviors relating to relideon or belief: Front of House staff or others reviewing CCTV footage may misinterpret behaviors or interactions among students/staff, potentially leading to misunderstandings or unwarranted interventions.

2B. cont'd - Please indicate potential positive, neutral and negative impacts in relation to each protected characteristic.

Protected Characteristic	Check the relevant box and provide an explanation for each option chosen, with reference to evidence, or information. Note: in some cases, impacts can be both positive and negative.		
Sex	Positive ☑ 1. Enhanced security: CCTV cameras can provide a sense of security for female students and staff, particularly in areas with high foot traffic or during late hours when safety concerns may be heightened. 2. Prevention of harassment and violence: CCTV surveillance may deter incidents of sexual harassment, assault, or other forms of violence against female students and staff, as perpetrators may be less likely to engage in such behavior if they know they are being monitored. 3. Documentation of incidents: CCTV footage can serve as valuable evidence in cases of harassment or violence against female students and staff, helping to hold perpetrators accountable and ensure justice.	Neutral ☑	Negative ☐ 1. Privacy concerns: Female students and staff may have concerns about their privacy being compromised by CCTV surveillance. 2. Fear of objectification: CCTV surveillance may exacerbate feelings of being objectified or judged based on appearance among female students and staff, as they may worry about being observed and scrutinized by others. 3. Fear of retaliation: Female students and staff who experience harassment or violence may be hesitant to report incidents if they fear that doing so will result in their actions being captured on CCTV and potentially used against them.
Sexual Orientation	Positive ☑ 1. Enhanced safety: CCTV cameras can help deter incidents of harassment, bullying, or violence against LGBTQIA+ students/staff, contributing to a safer campus environment. 2. Documentation of incidents: CCTV footage can serve as evidence in cases of discrimination or hate crimes targeting LGBTQIA+ individuals, facilitating investigations and ensuring accountability.	Neutral ☐	Negative ☑ 1. Privacy concerns: LGBTQIA+ students/staff may have concerns about their privacy being compromised by CCTV surveillance, 2. Fear of exposure: LGBTQIA+ students/staff who are not out may fear being inadvertently outed if they are observed engaging in affectionate behavior or socializing with same-sex partners in CCTV footage that is reviewed by others. 3. Stigmatization: LGBTQIA+ students may feel stigmatized or singled out by the presence of CCTV cameras, particularly if they wrongly perceive the surveillance as monitoring their behavior or relationships based on their sexual orientation. 4. Impact on mental health: CCTV surveillance can contribute to feelings of anxiety, paranoia, or discomfort among LGBTQIA+ students/staff, especially if they perceive the cameras as intrusive or judgmental.

Step 3: Consider Alternatives and Mitigation	
3A. Are you able to reduce any potential negative impacts identified above?	
Yes: ☑ No: ☐	**For 3B and 3C, please detail relevant protected characteristics and refer to evidence/information.** **Note: In some cases, both "yes" and "no" may be suitable responses.**
3B. If "Yes", what arrangements could be implemented to reduce any potential negative impacts identified above? 1. Ensuring that CCTV systems are positioned and configured to minimize privacy intrusions and accessibility barriers. 2. Providing clear guidelines and procedures for accessing CCTV footage in a manner that respects the privacy and dignity of students/staff with protected characteristics. 3. Providing training to Front of House Officers on interacting with students/staff with protected characteristics and accommodating their specific needs in emergency situations. 4. Engaging with student/staff networks to gather feedback and address concerns related to the use of CCTV on campus. .	
3C. If "No", it may be appropriate if the policy, procedure, or relevant practice affects groups differently where this is a proportionate means of achieving a legitimate aim. If this is the case, please provide explanatory details to objectively justify this decision. (Note: you may be required to obtain legal advice to verify your decision. If you suspect this may be the case, please contact Equality, Diversity & Inclusion for direction.	

Step 4: Compliance with the Public Sector Equality Duty (PSED)

4A. Does the policy, procedure or relevant practice comply with the three parts of the PSED?

- **Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by the Act.**
- **Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.**
- **Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.**

Yes: ☑ No: ☐	**For 4B- 4D, please detail relevant groups who share a protected characteristic and refer to evidence/information.** **Note: In some cases, both "yes" and "no" may be suitable responses.**

4B. If "Yes", how?

1. Enhanced security, will create a safe enviroment for all people who share a protected charateristic and those who do not.
2. Prevention of harassment and violence, creating a safe enviroment for all staff and students.
3. Documentation of incidents to support staff and students that may have faced harrassment, bullying or discrimination.

The policy complies with the three parts of the PSED where the CCTV Code of Practice is relevant.

4C. If "No", what are the negative impacts and the associated risks?

4D. If "Yes" or "No", what changes could be implemented to better comply with the PSED?

Step 5: The Involvement of Individuals, Groups and Organisations Representing Protected Characteristics

5A. Who has been involved in the undertaking of this assessment?
(Please detail the staff/student/stakeholder groups, in particular those representing protected characteristics)

Associate Director People & Culture
EDI Manager
Head of Student Support & Wellbeing
Learning Support Manager
Data protection Officer

5B. If you have further involvement to carry out, please list who you are going to involve, when and why?

Step 6: Making a decision and outcome

6A. What is your decision? **(Please select an option from below)**

A. A positive impact is explicitly intended and very likely. ☐

B. A negative impact is not expected. There is clear potential to have a positive impact by minimising or eliminating barriers and inequalities that currently exist. ◯

C. A negative impact is not expected, but positive impact is also unlikely. ◯

D. A negative impact is probable or certain for some groups but the policy as a whole can nevertheless be justified as a proportionate means of achieving a legitimate aim. ◯

(Note: you may be required to obtain legal advice to verify your decision. If you suspect this may be the case, please contact Equality, Diversity & Inclusion for direction.)

6B. Are you able to introduce the policy, procedure, or relevant practice without making any changes?	Yes: ☐ No: ◯

6C. If "Yes", clearly explain upon which basis this decision was made

The Code of Practice is to ensure the safety of staff and students without infringing on their rights. As stated consideration is given to the position of the cameras whilst ensuring that privacy and dignity is crucial to how this is managed. Staff training and consultation with staff and students will be ongoing. It was may also provide camera footage of any potential incidents of bullying or harrassment, therefore supporting those with protected charaterisitcs.

6D. If "No", what changes will you make before implementation?

Step 7: Taking action and monitoring

7D. Once implemented, how will the policy, procedure, or relevant practice be monitored, by whom and by when?

The CCTV Code of Practive will be published on MyConnect with a review date. This will be monitored by the Performance team and reviewed by the Associate Director, People & Culture when necessary. Should any updates be required, due to change in process, changes to legislation or changes to lines of responsibility, this will be updated and a review of the EQIA conducted.

Step 8: Approval and Publishing	
• **The information contained within this EqIA needs to be confirmed and approved as the completed EqIA will be published on the College web-site.** • **As such, EqIAs must be approved by a Dean/Director or above.** • **Following completion, send the electronic copy to both the Quality Unity Administrator and the Equality, Diversity & Inclusion Manager.** • **An electronic signature is acceptable, as long as a scanned or paper copy follows.**	
Name:	John Gribben
Position:	Vice Principal, People & Corporate Support
Signature:	John Gribben
Date:	3/5/24

Miscellaneous
Please insert any supporting information, evidence sources, or data here.

Summary of the Public Sector Equality Duty (PSED) of the Equality Act 2010

Components A public authority must, in the exercise of its functions, have **due regard** to the need to:	**Due Regard** Having due regard specifically involves taking steps to:
a) Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by the Act. **(Fairness)**	
b) Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it. **(Opportunity)**	a) Remove or minimise disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic * b) Take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it. c) Encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.
c) Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. **(Respect)**	a) Tackle prejudice. b) Promote understanding.

'Due regard' comprises two linked elements: proportionality and relevance. The weight that public authorities give to equality should be proportionate to how relevant a particular function is to equality. In short, the more relevant a policy, procedure or practice is to equality and people, then the greater the regard that should be paid.

The protected characteristics are:

- **Age**
- **Disability**
- **Gender reassignment**
- **Marriage and Civil Partnership ***
- **Pregnancy and Maternity**
- **Race**
- **Religion or Belief**
- **Sex**
- **Sexual Orientation**

*** Although Marriage and Civil Partnership applies to section a) in employment only, this will be considered for all stakeholders.**