POLICY / PROCEDURE TITLE		DATE OF APPROVAL
CCTV Policy		May 2024
APPROVED BY	**VERSION NO.**	**VALID UNTIL**
Executive Board	1	May 2027

OWNER	Director of Assurance & Risk		
GROUP EXECUTIVE LEAD	Chief Finance Officer		
DOCUMENT TYPE	Policy ☒	Group Procedure ☐	Local Procedure ☐
PURPOSE	NCG's use of CCTV and Body Worn Video (BWV) is covered by the UK General Data Protection Regulation (GDPR). Identifiable imagery is considered as personal data under the UK 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 and BWV will be dealt with lawfully and correctly in accordance with NCG's Data Protection Policy.		
APPLICABLE TO	All NCG employees, as well as consultants, vendors, agency workers, contractors, service users, trainees/students, volunteers and/or any other parties who use/access NCG premises.		
EQUALITY ANALYSIS COMPLETED [POLICIES ONLY]	Yes ☒	No ☐	N/A ☐
	(If EA not applicable, please explain)		
KEY THINGS TO KNOW ABOUT THIS POLICY	1. Identifiable imagery is considered as personal data under the UK GDPR and, therefore, this policy is committed to the protection of individuals' rights and privacy. 2. This policy informs users of NCG premises of the arrangements for the placement and management of CCTV and BWV.		
EXPECTED OUTCOME	Readers are expected to understand the organisational position on NCG's use of CCTV and BWV, know their responsibilities in relation to the policy and comply with the terms of the policy.		

MISCELLANEOUS	
LINKED DOCUMENTS	• Data Protection Policy • Information Governance Policy • Staff Privacy Notice

	• Learner Privacy Notice • Data Retention Schedule
KEYWORDS	• Closed Circuit Television cameras (CCTV) • Body Worn Video (BWV) • UK GDPR • Data Protection Act 2018

Equality Impact Assessment

EQUALITY IMPACT ASSESSMENT			
	Yes	**No**	**Explanatory Note if required**
EIA 1 - Does the proposed policy/procedure align with the intention of the NCG Mission and EDIB Intent Statement in Section 2?	☒	☐	The answer to this must be YES
EIA 2 - Does the proposed policy/procedure in any way impact unfairly on any protected characteristics below?	☐	☒	
Age	☐	☒	The answer to this must be NO
Disability / Difficulty	☐	☒	The answer to this must be NO
Gender Reassignment	☐	☒	The answer to this must be NO
Marriage and Civil Partnership	☐	☒	The answer to this must be NO
Race	☐	☒	The answer to this must be NO
Religion or Belief	☐	☒	The answer to this must be NO
Sex	☐	☒	The answer to this must be NO
Sexual Orientation	☐	☒	The answer to this must be NO
EIA3 - Does the proposed policy/processes contain any language/terms/references/ phrasing that could cause offence to any specific groups of people or individuals?	☐	☒	The answer to this must be NO
EIA4 - Does the policy/process discriminate or victimise any groups or individuals?	☐	☒	The answer to this must be NO
EIA 5 - Does this policy/process positively discriminate against any group of people, or individuals?	☐	☒	The answer to this must be NO
EIA 5 - Does this policy/process include any positive action to support underrepresented groups of people, or individuals?	☐	☒	The answer to this could be yes or no as positive action is lawful. However, an explanation must be provided for clarity.
EIA 6 - How do you know that the above is correct?	This policy has been reviewed by the NCG Executive Board.		

1. INTRODUCTION

NCG is committed to providing a safe and secure learning environment across its campuses and buildings. NCG therefore operates Closed Circuit Television cameras (CCTV) across its campuses and buildings for the security and safety of its staff and students. CCTV cameras are installed to view and record the activities of individuals overtly at selected locations on NCG premises.

NCG also utilises Body Worn Video (BWV) for security purposes. BWV involves the use of video cameras that are worn by a person and are often attached onto the front of clothing or a uniform. The principles outlined within this policy apply to BWV also.

The deployment of these BWV and CCTV cameras is a strategic component of NCG's commitment to staff and student safety, security, and crime prevention.

The use of CCTV and BWV is covered by the UK General Data Protection Regulation (GDPR). Identifiable imagery is considered as personal data under the UK 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 and BWV will be dealt with lawfully and correctly in accordance with NCG's Data Protection Policy.

2. THE CCTV SYSTEM AND BWV

The CCTV systems adopted across NCG vary depending on the specific requirements and provisions at each campus, but the equipment includes internal / external; static colour / black and white; full pan, tilt and zoom cameras.

The vast majority of CCTV cameras are Internet Protocol (IP) based and connected to the NCG IT network. The system records CCTV data in real time to specific Networked Video Recorders (NVR) in secure locations across the NCG estate. For buildings where analogue CCTV system is in use, the camera output is cabled to Video Camera Recorders (VCR's) with real time recording available on motion sensors. The output of the cameras can be relayed between the VCR's and authorised desktop computers via web links on NCG's computer network.

The BWV used at NCG can record both video and audio when the BWV is in use. In line with UK GDPR, video and audio is recorded on BWV only in circumstances where NCG can justify the recording of both audio and video together.

The Executive member responsible for BWV and the CCTV system is the Chief Information, Data and Estates Officer. NCG is the owner of all recorded CCTV and BWV data.

3. PURPOSE OF THE SYSTEM

The purpose of the CCTV system and BWV is as follows:

- Facilitate the safety of staff, students, contractors, and visitors.
- Provide an effective means by which to prevent and reduce crime in the monitored areas through an increased fear of detection and the prevention of offenders.
- Assist in the factual, accurate and speedy reconstruction of the circumstances of incidents.
- To assist NCG and police in providing a swift response to criminal activity and provide evidential material for court and disciplinary proceedings.
- Protect NCG's assets.
- To assist in traffic management within NCG's car parks.
- To assist in supporting NCG's Health and Safety policies.
- To assist in the event of an emergency or disaster.

4. SCOPE

The CCTV system is intended to view, monitor, and record activities within NCG's premises. It will focus primarily, but not limited to, key entry and exit points to premises, building perimeters, certain communal areas and other parts where CCTV is recommended to mitigate against risks to safety and security.

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

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

The system will be operated fairly to ensure that all BWV and CCTV data is processed in accordance with UK GDPR, the Data Protection Act 2018 and the NCG Data Protection Policy and only for the purposes to which it is established.

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

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

BWV records both video and audio therefore, the BWV should be switched on and off as required to ensure that excessive information is not recorded continuously.

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

5. SIGNAGE

Strategically placed CCTV camera notices at key entry points to NCG premises should be in place to advise individuals that they are entering an area which is covered by CCTV cameras.

The CCTV notice at entrances to NCG premises and in adjacent areas will contain:

- The name of the Data Controller (i.e. NCG).
- The purpose(s) of the scheme.
- A contact name and telephone number for enquiries.

For BWV, there is an expectation that we will verbally inform or verbally announce to individuals that the recording of video or audio or both is about to take place, and the reasons why, prior to turning on the BWV device. Further, we should have in place visible signage or a warning light on the device or uniform, to indicate that the device is switched on and recording.

6. CAMERA LOCATIONS

The CCTV systems installed in and around the NCG estate comprise of a mixture of fixed and pan / tilt / zoom cameras. These cameras provide fields of view encompassing approaches to building entrances, building property lines and

internal communal and secure areas. Where external and internal blind spots have been identified, this should be logged at each site.

Covert cameras are not installed anywhere on NCG premises. However, NCG reserves the right to deploy covert cameras in exceptional circumstances affecting public safety, prevention and apprehension of nefarious and criminal activities within the premises. Any deployment of covert cameras will require written approval from either a member of the Executive team, the Data Protection Officer or law enforcement agencies.

BWV is a portable system that are worn by a person and are often attached onto the front of clothing or a uniform.

7. DATA PROTECTION

This policy document will be implemented to ensure that the deployment and control of BWV and CCTV resources is proportionate and lawful under the terms of the UK General Data Protection Regulations (GDPR), the Data Protection Act 2018 and the CCTV Codes of Practice issued by the Information Commissioner Office (ICO).

In summary, personal data should be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. It requires that appropriate technical or organisational measures are used.

The lawful basis identified for processing the personal data as part of the BWV and CCTV system is legitimate interest.

This CCTV Policy should be read in conjunction with the following policy documents:

- NCG Data Protection Policy.
- Staff and Learner Privacy Notices.
- Data Retention Schedule.

8. RESPONSIBILITIES

NCG as owner has responsibility for compliance with the purposes and objectives of the system including operational guidance and the protection of the interests of

NCG users and privacy of the individuals whose images are captured on the system.

This responsibility is undertaken by the following members of staff:

Data Protection Officer

The Director of Assurance & Risk is the appointed Data Protection Officer responsible for the management of data protection matters and for the development of specific guidance and practice on data protection issues for NCG.

Director of Estates

The Director of Estates shall have responsibility for both BWV and the CCTV infrastructure, ensuring there is an adequate maintenance regime and upgrades to BWV and CCTV hardware and software, so they are fit for purpose. The Director will support the Heads of Estates in developing and maintaining appropriate BWV and CCTV data processing and handling practices within NCG in accordance with the Data Protection Policy.

Heads of Estates

The Heads of Estates are responsible for the day-to-day management and control of the BWV and CCTV system on behalf of NCG. Where management of the CCTV system is part of an outsourced contract, they will work closely with the outsourced provider to ensure service and maintenance agreements are carried out as dictated by the respective contract or industry standard. The Heads of Estates will work with the providers of security services and CCTV contracts, to create an awareness of the data protection responsibilities of security staff.

Director of IDS

The Director of IDS is responsible for protecting data on NCG's IT systems and will ensure there are appropriate technical and organisational security measures in place to protect BWV and CCTV data on the system.

9. ASSESSMENT OF THE POLICY

The Heads of Estates will evaluate the system periodically to consider the following (in conjunction with colleagues listed in Section 8 above):

- 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 exists.
- Future functioning, management, and operation of the system.

10. MANAGEMENT OF THE SYSTEM

The Director of Estates is responsible for the management of NCG's BWV and CCTV system. This includes the maintenance and operation of the system as well as the protection of the privacy interests of individual members of NCG and the public from intrusive monitoring.

The Director of Estates (in conjunction with the Heads of Estates) will ensure that all Security staff involved in the recording, observation and capture of images are informed, through training on operating BWV and the CCTV system or through other means, of their responsibility to act in an ethical and lawful manner in line with relevant legislation and industry standards.

For the purpose of viewing BWV and CCTV images, an authorised person is defined as an employee or appointed person acting on behalf of NCG who has an operational responsibility for either the prevention, investigation or detection of crime and / or the monitoring of the security and safety of NCG premises.

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

11. ACCESS TO CCTV MONITORS AND MONITORING EQUIPMENT

CCTV monitors which display live images may be installed in public areas to show live images of activities in the area. This may be deployed when it is important to emphasise an area is under CCTV surveillance as a deterrent to criminal activities, antisocial behaviour or allay any safety concerns within the area. The monitor displays only a scene or live image which is also in plain sight from the monitor location. Unless specifically designed for these purposes, access to CCTV

monitors or display screens will be restricted to persons authorised to view those images.

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

Where software application allows remote access to the system for authorised staff via the web link, access rights to the systems will be secure.

12. RECORDING AND STORAGE OF INFORMATION

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

CCTV / BWV data is not to be retained for longer than necessary. Data storage is automatically managed by the CCTV digital recorders which use a software programme to overwrite historical data in chronological order to enable the recycling of storage capabilities.

Data storage is also automatically managed by the management systems used to store footage from BWV.

Provided that there is no legitimate reason for retaining BWV footage and the CCTV images (such as for use in legal or disciplinary proceedings), the images / footage will be erased following the expiration of the retention period associated with the specific system (typically one calendar month for CCTV images and five working days for BWV footage). Where the retention period associated with the specific system differs from one calendar month for CCTV or five working days for BWV footage and cannot be adjusted, the retention period should be documented for clarity.

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

Access to BWV and the CCTV system and to the captured images and audio will be restricted to authorised staff involved in monitoring or investigation.

Authorised staff include:

- Principalship / Executive teams or appointed investigating managers for the purposes of conducting an investigation / reviewing an incident on college campus.

- Director of Estates, Heads of Estates and Security colleagues for the purposes of reviewing the effectiveness of BWV and CCTV operations and for conducting surveillance / reviewing footage in the event of an incident / potential criminal activity.
- Data Protection Officer (where consultation from a data protection perspective is required).

13. ACCESS AND DISCLOSURE OF BWV FOOTAGE AND CCTV IMAGES

Requests for access to (review), or disclosure of (i.e. provision of a copy) images recorded on the CCTV systems or BWV footage 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 or audio have been recorded by the CCTV systems/ BWV).
- Law enforcement agencies (where the audio and images recorded would assist in a specific criminal enquiry).
- Prosecution agencies (including NCG management in the course of staff or student disciplinary proceedings).
- Relevant legal representatives of data subjects.

Images / footage from CCTV and BWV **must not** be forwarded to the media for entertainment purposes or be placed on the internet.

Images / footage will only be released to the media on the authority of the Executive (in conjunction with the Data Protection Officer) and following advice from law enforcement agencies to support police investigations.

With regard to the right of access, staff, students and other data subjects about whom NCG holds or uses personal data have a legal right to access that information and can 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: dpo@ncgrp.co.uk. An electronic copy of the Data Subject Access Form can be obtained from NCG’s website or requested by email from dpo@ncgrp.co.uk.

By law, NCG has one month from receipt of the request along with proof of identity, in which to respond to subject access requests. In any event NCG will endeavor to respond as quickly as possible. In limited circumstances, NCG 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.

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 (along with the appropriate ID of the data subject).

NCG has the discretion to refuse any third-party request for information unless there is an overriding legal obligation such as a court order or information access right. 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.

It may be necessary for redaction of images on copies of CCTV or BWV footage issued following a subject access request. This is usually to protect third party data. Where redaction is deemed impossible for example large video files or due to lack of functionality to do this, NCG may refuse a BWV or CCTV data request if providing this data, infringes on the rights to privacy of others (in these instances we may invite third parties to view the information rather than disclose to avoid infringing the rights of others). All instances of this should be discussed with the Data Protection Officer to ensure the correct course of action is taken.

When recorded CCTV images or BWV footage is viewed or a copy of data is released to authorised persons/organisation, a log must be maintained and signed by the issuer and requestor.

All disclosed BWV and CCTV data must be delivered in an appropriately secure manner (which can be agreed with the Data Protection Officer).

The ICO website provides further information on the above rights (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access). The NCG Data Protection Officer can also be contacted via dpo@ncgrp.co.uk.

14. LIAISON WITH THE POLICE (OR OTHER LAW ENFORCEMENT AGENCIES)

Images and footage may be released to the Police Service or other law enforcement agencies in compliance with Police Act 1996, the Data Protection Act 2018 and UK GDPR.

When BWV and CCTV data requests are received from the Police Services or other law enforcement agencies, they must provide their standard issued badge as proof of identity, the purpose of the request (e.g. the prevention / detection of a crime) and provide signatures for any BWV and CCTV footage/ images collected.

All CCTV and BWV data viewed or released to the police must be logged in the law enforcement access request register (maintained by the Data Protection Officer).

15. INSTALLATION

The CCTV installations are carried out through consultation with external CCTV providers approved by NCG.

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.

NCG reserves the right to deploy/restrict/cease the use of dummy cameras as part of the system subject to applicable laws, ICO code of practice or police directive.

16. CRIMINAL OFFENCE DATA

All security staff involved in the recording, observation and capture of images and audio (on BWV) must act in an ethical and lawful manner in accordance with legislation and must receive adequate training to ensure their understanding of compliance legislation.

The CCTV policy as with all other NCG policies and procedures are deemed reasonable management instructions covered by an employee's contract of employment. As a result, breaches of any aspect of this policy may result in disciplinary penalties or be referred to the police as the subject of criminal or civil offence investigation.

17. COMPLAINTS

All complaints and enquiries relating to the CCTV system should be addressed to: NCG, Rye Hill House, Scotswood Road, Newcastle Upon Tyne, NE4 7SA or via the complaints mailbox: NCGComplaints@ncgrp.co.uk.

18. BREACHES OF POLICY

Breaches of the policy and of security will be investigated by the Director of Estates or the Data Protection Officer (or nominee). Recommendations and corrective action plans will be put in place to remedy any breach which is proven.
The Data Protection Officer is responsible for maintaining a record of CCTV data breaches as part of the policy.

All breaches of personal data must be reported to the Data Protection Officer via dpo@ncgrp.co.uk.

19. STATEMENT ON IMPLEMENTATION

Upon approval, this policy will be uploaded to the policy portal and communicated to staff via The Business Round-Up.
List any additional measures needed to ensure the policy is implemented and any training that may be available.

20. STATEMENT ON EQUALITY AND DIVERSITY

NCG is committed to providing equality of opportunity. Further details or our aims and objectives are outlined in our Equality Diversity Inclusion and Belonging Strategy.
This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly. In applying this policy, we have considered eliminating unlawful discrimination, promoting equality of opportunity and promoting good relations between people from diverse groups.

21. STATEMENT ON CONSULTATION

This policy has been reviewed in consultation with Policy Review Council prior to approval from Executive Board.

VERSION CONTROL				
Version No.	**Documentation Section/Page No.**	**Description of Change and Rationale**	**Author/Reviewer**	**Date Revised**
1	New Policy	N/A	Director of Assurance & Risk	April 2024

APPENDIX A

Request For CCTV / BWV Footage Release under Schedule 2 Paragraph 2 of the Data Protection Act 2018 for Crime and Taxation

SECTION 1A – APPLICANT DETAILS TO BE COMPLETED BY THE POLICE

Surname:		**Rank:**	
Forename(s):		**I.D. Number:**	
Station Address:		**Work Telephone Number:**	

SECTION 1B – APPLICANT DETAILS TO BE COMPLETED BY LAW ENFORCEMENT AGENCIES AND LEGAL REPRESENTATIVES

Surname:		**Agency Name:**	
Forename(s):		**Agency Type:**	
Registered Legal Address:		**Work Telephone Number:**	

SECTION 2 – DETAILS OF DATA REQUIRED

Date of Incident:	Area/Camera Location:	Approximate Time:

Details of Incident:

SECTION 3 – JUSTIFICATION

This CCTV / BWV footage is requested under Schedule 2, Paragraph 2 of the Data Protection Act 2018 for the following reasons:

(Place an X in the appropriate box)

[ ] The prevention or detection of crime

[ ] The apprehension or prosecution of offenders

[ ] The assessment or collection of a tax or duty or an imposition of a similar nature

Please provide further details (explain why the information is needed and what the impact would be in the event of non-disclosure):

SECTION 4 – DECLARATION STATEMENT

I *(please print name*) _____
confirm that:

- I wish to obtain CCTV / BWV footage under Schedule 2, Paragraph 2 of the Data Protection Act 2018.
- The data hereby requested will be kept in a secure location at

  _____

  _____

  with access solely to those officers/individuals involved in the specific investigation.
- Any footage disclosed to me will only be used for the purpose(s) specified in Section 3 of this request form.

Once the footage has been used for the purpose(s) specified in Section 3 and the investigation is complete, the footage will be confidentially destroyed by the body that is requesting this footage.

Signature: _____

Date: _____

Please return form to [college to enter relevant contact details]

Internal Office Use Only:

Date request received:

Will the footage be released?

[ ] Yes

[ ] No

Reason for refusal:

Date completed:

Signature:

Print name:

APPENDIX B

Data Subject Request Form for the Release of CCTV / BWV Footage

SECTION 1 – APPLICANT DETAILS

Full Name:	
Email Address:	
Contact Number:	
Home Address:	

Are you the data subject – Please place an X in the appropriate box and read the instructions that follow:

☐ **Yes** - I am the Data Subject. I enclose proof of my identity.

☐ **No** - I am acting on behalf of the data subject. I have enclosed the data subjects written authority and proof of the data subjects identity and my own identity (see below).

Identification

For verification purposes, we require you to provide us with proof of your/ your client's identity and address.

Please supply us with a photocopy or scanned image of one or more of the following to confirm your identity and address:

- Proof of identity – Such as passport, photo driving licence, national identity card, or birth certificate.

- Proof of address – Such as a utility bill, bank statement, credit card statement (dated within the last 3 months), current driving licence, current TV licence, local authority tax bill, or HMRC tax document (dated within the last 12 months).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 2 – DETAILS OF DATA REQUIRED

Date of Incident:	Area/Camera Location:	Approximate Time:
Details of the Incident:		

SECTION 3 – JUSTIFICATION

Under data protection legislation, NCG have an obligation to protect the confidentiality of other individuals. Before we release the CCTV / BWV footage to you, we will review it to determine whether it contains footage of any other individual. Where this is the

case, we may not be able to release the footage unless you have a reasonable justification for requiring it. Please state your justification in the box below, as well as any Crime Incident Number where applicable:

Crime Incident Number (if applicable):	
Justification:	

SECTION 4 – DECLARATION STATEMENT

I *(please print name*) _____
confirm that:

- The information provided on this application form is true.
- I understand that it is necessary for NCG to confirm my identity and it may be necessary to obtain more information in order to locate the correct information.
- Any CCTV / BWV footage disclosed to me will only be used for the purpose(s) specified in section 3 of this request form.
- Where CCTV/ BWV footage has been provided directly to the data subject, I will return the CCTV/ BWV footage to the Security Team within 14 days to ensure the footage can be confidentially destroyed. Where I have a justified reason to hold the footage for longer than the 14-day release period and the Security Team have agreed this, I will return the footage to Security Team in line with agreed timeframes.
- Where CCTV/ BWV footage has been provided to you as legal representative on behalf of the data subject, I will ensure once the footage has been used for the purpose(s) specified in Section 3 and the investigation is complete, the footage will be confidentially destroyed.

Signature: _____

Date: _____

Please return form to [college to enter relevant contact details]

Internal Office Use Only:

Date request received:

Will the footage be released?

[ ] Yes

[ ] No

Reason for refusal:

Date completed:

Signature:

Print name: