INTRODUCTION
Closed Circuit Television (CCTV) is already installed in NCG Manchester. New CCTV systems will be introduced in consultation with staff and the board of management. Where systems are already in operation, their operation will be reviewed regularly in consultation with staff and management.

1. PURPOSE OF POLICY

The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of NCG.

CCTV systems are installed for the purpose of enhancing security of the building and its associated equipment as well as creating mindfulness among the occupants, at any one time that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance at NCG is intended for the purposes of:
- protecting the college buildings and college assets, both during and after college hours;
- promoting the health and safety of staff, students and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- Ensuring that the college rules are respected so that the college can be properly managed.

2. SCOPE

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried out in rented premises, NCG will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

3. GENERAL PRINCIPLES

NCG as a corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. NCG owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the college community by integrating the best practices governing the public and private surveillance of its premises. The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.
Information obtained through the CCTV system may only be released when authorised by the Principal or Managing Director. Any requests for CCTV recordings/images from NCG will be fully recorded and legal advice will be sought if any such request is made. (See “Access” below). If a law enforcement authority, is seeking a recording for a specific investigation, NCG may require a warrant and accordingly any such request made should be requested in writing and NCG will immediately seek legal advice.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by NCG, including Equality & Diversity Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within college/ETB premises is limited to uses that do not violate the individual’s reasonable expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of NCG or a student attending one of its colleges/centres. All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by NCG. Recognisable images captured by CCTV systems are “personal data.” They are therefore subject to the provisions of the Data Protection Acts 1988 and 2003.

4. JUSTIFICATION FOR USE OF CCTV

Section 2(1)(c)(iii) of the Data Protection Act requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that NCG needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to control the perimeter of the college buildings for security purposes has been deemed to be justified by the board of management. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

**CCTV systems will not be used to monitor normal teacher/student classroom activity in college.**

In other areas of the college where CCTV has been installed, e.g. hallways, stairwells, locker areas, the Managing Director has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.
5. LOCATION OF CAMERAS
The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. NCG has endeavoured to select locations for the installation of CCTV cameras which are the least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recordings may include the following:

- **Protection of college buildings and property:** The building’s perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas
- **Verification of Security Alarms:** Intrusion alarms, exit door controls, external alarms
- **Criminal Investigations:** Robbery, burglary and theft surveillance

6. COVERT SURVEILLANCE
NCG will not engage in covert surveillance.

7. NOTIFICATION – SIGNAGE
The Principal will provide a copy of this CCTV Policy on request to staff, students and visitors to the college. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Board of Management. Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to NCG. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Appropriate locations for signage will include:
- at entrances to premises i.e. external doors, college entrances
- reception area
- at or close to each internal camera

8. STORAGE & RETENTION
Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.
Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Principal. The Principal may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Police, the Deputy Principal, the relevant members of the teaching staff, representative of the HSE, a student and/or the parent of a recorded student. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Any saved footage will be stored in a secure environment with a log of access. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

9. **ACCESS**

Storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Principal of college

In relevant circumstances, CCTV footage may be accessed:

- Where NCG are required by law to make a report regarding the commission of a suspected crime; or

- Following a request when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on NCG property, or

- To the HSE and/or any other statutory body charged with child safeguarding; or

- To assist the Principal in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians/student will be informed; or

- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to NCG or

- To individuals (or their legal representatives) subject to a court order.
To the college’s insurance company where the insurance company requires the same in order to pursue a claim for damage done to the insured property.

Information obtained through video monitoring will only be released when authorised by the Principal following consultation with the Managing Director. If the police request CCTV images for a specific investigation, it may require a warrant and accordingly any such request made by the police should be made in writing and the college should immediately seek legal advice.

A person should provide all the necessary information to assist NCG in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the college.

In giving a person a copy of their data, the college may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

10. RESPONSIBILITIES
The Principal will:
- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by NCG
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within NCG
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at NCG is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to, or the release of tapes, or any material recorded or stored in the system
- Ensure that footage is not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally

NCG will also when required to do by law
- Provide a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment, located in NCG
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the college and be mindful that no such infringement is likely to take place

Version 1 January 2016 | Revision date January 2017 |
• Co-operate with the Health & Safety Officer in reporting on the CCTV system in operation in the college
• Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”
• Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only

11. IMPLEMENTATION and REVIEW
The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner)
APPENDIX 1 - DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All college staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including:
- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.