Norbury Manor Business & Enterprise College *for* Girls

CCTV Policy

Next review date: **June 2020**

Staff resp. for review: **WK / ARO**

Date reviewed: **June 2019**

CCTV POLICY

1 Policy Statement

1.1 Norbury Manor uses Closed-Circuit Television ("CCTV") within the premises of the college. The purpose of this policy is to set out the position of the college as to the management, operation and use of the CCTV at the college.

1.2 This policy applies to all members of our workforce, visitors to the college premises and all other persons whose images may be captured by the CCTV system.

1.3 This policy takes account of all applicable legislation and guidance, including:

1.3.1 General Data Protection Regulation ("GDPR")

1.3.2 Data Protection Act 2018 (together the Data Protection Legislation)

1.3.3 CCTV Code of Practice produced by the Information Commissioner

1.3.4 Human Rights Act 1998

1.4 This policy sets out the position of the college in relation to its use of CCTV.

2 Purpose of CCTV

2.1 The college uses CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for students, staff and visitors – the CCTV supports safeguarding but does not provide full coverage

2.1.2 To prevent the loss of or damage to the college buildings and/or assets

2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

2.1.4 To monitor behaviour of students and conduct of staff and visitors

3 Description of system

3.1 There are 128 cameras across the college site. All internal and 10 external cameras are fixed. There are also 8 external PTZ (Pan Tilt & Zoom). They do not have sound recording capabilities.

4 Siting of Cameras

4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, students and visitors.

4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The college will make all reasonable efforts to ensure that areas outside of the college premises are not recorded.

4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

4.4 Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilet cubicles.

5 Privacy Impact Assessment (see Appendix 1)

5.1 Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the college to ensure that the proposed installation is compliant with legislation and ICO guidance.

5.2 The college will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and Access

6.1 The CCTV system will be managed by D Heavens (premises manager) and P. Harris (network manager)

6.2 On a day to day basis the CCTV system will be operated by the site staff

6.3 The viewing of live CCTV images will be restricted to the site staff, pastoral staff, reception staff (safeguarding) and SLT

6.4 Recorded images which are stored by the CCTV system will be restricted to access by site staff, reception staff, SLT and heads of year

6.5 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images

6.6 The CCTV system is reviewed annually by site staff and the network manager to ensure that it is operating effectively

7 Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

7.2 Recorded images are stored only for a period of 28 daysunless there is a specific purpose for which they are retained for a longer period.

7.3 The college will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

7.3.1 CCTV recording systems being located in restricted access areas;

7.3.2 The CCTV system being password protected;

7.3.3 Restriction of the ability to make copies to specified members of staff

7.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the college.

8 Disclosure of Images to Data Subjects

8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.

8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the college's Subject Access Request Policy.

8.3 When such a request is made the premises staff and network manager will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

8.4 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The premises manager and network manager must take appropriate measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals then the college must consider whether:

8.5.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

8.6 A record must be kept, and held securely, of all disclosures which sets out:

8.6.1 When the request was made;

8.6.2 The process followed by the network and premises manager in determining whether the images contained third parties;

8.6.3 The considerations as to whether to allow access to those images;

8.6.4 The individuals that were permitted to view the images and when; and

8.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

9 Disclosure of Images to Third Parties

9.1 The college will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

9.3 If a request is received form a law enforcement agency for disclosure of CCTV images then the premises and network managers must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

9.4 The information above must be recorded in relation to any disclosure.

9.5 If an order is granted by a court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10 Review of Policy and CCTV System

10.1 This policy will be reviewed annually.

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed annually.

11 Misuse of CCTV systems

11.1 The misuse of CCTV system could constitute a criminal offence.

11.2 Any member of staff who breaches this policy may be subject to disciplinary action.

12 Complaints relating to this policy

12.1 Any complaints relating to this policy or to the CCTV system operated by the college should be made in accordance with the college complaints policy.

APPENDIX 1: CCTV PRIVACY IMPACT ASSESSMENT

1 Who will be captured on CCTV?

Students, staff, parents / carers, volunteers, governors and other visitors including members of the public

2 What personal data will be processed?

Facial Images, behaviour, sound, safety

3 What are the purposes for operating the CCTV system? .

Cameras are used to monitor activities within college buildings, on its sites, its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived. CCTV is also used for the purpose of monitoring the behaviour of students and conduct of staff and visitors, supporting the safety and well being of the college, together with its staff, students and visitors.

4 What is the lawful basis for operating the CCTV system?

Legal obligation: legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime Public Task

5 Who is/are the named person(s) responsible for the operation of the system?

Mr D Heavens – site manager Mr P Harris – network manager Caretaking and site team

6 Describe the CCTV system, including:

a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;

b. siting of the cameras and why such locations were chosen;

c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

a. maintained by a contracted security company annually
b. all CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated: cameras are sited in prominent positions so as to be evenly spread across the college site
c. cameras are sited in prominent positions where they are clearly visible to all staff students and visitors; they are not sited in areas where individuals have a heightened expectation of privacy such as changing rooms
d. signs will be erected to inform individuals that they are in an area where CCTV is in operation – these are generally areas where there are often large numbers of students, near lockers which may contain valuables or near classrooms containing expensive equipment – they are also sited in places which are considered to be less visible
e. the system does not have a blurring function
The CCTV system is designed to ensure maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

7 Set out the details of any sharing with third parties, including processors

Access to the college's CCTV system is only available with consent from the head teacher and senior leadership team.
CCTV recorded images may be viewed by the police for the prevention and detection of crime, authorised staff of the college for supervisory purposes, discipline reasons or authorised demonstration and training.

8 Set out the retention period of any recordings, including why those periods have been chosen

Our recording period ranges between 2-4 weeks - the length of storage available on our system

9 Set out the security measures in place to ensure that recordings are captured and stored securely

Limited access to CCTV Log book kept of all requests which go through SLT

10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

For example: • Staff, students and visitors are recorded to ensure their health and safety • Recordings are deleted in 4 weeks minimising the amount of data being processed • The CCTV is in an office room which is either manned or locked. • Potential risks are: unlawful access • Risks during any transfer of recordings to third parties such as the police are how long they retain them for and where they store the data

11 What measures are in place to address the risks identified?

Assessing checks in place regarding access and log book Consider discussing CCTV with parents – include in IT agreement and code of conduct Check security of CCTV office Discuss retention with third parties

12 Have parents and students where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

When set up but not recently

13 When will this privacy impact assessment be reviewed?

June 2020

Approval:

This assessment was approved by the Data Protection Officer:

DPO A Ryder Owen

Date 07/06/19