CCTV Policy

Introduction

1. The NFTS ('the School') is committed to providing a safe and secure learning environment across its site. The School therefore operates close circuit television cameras (CCTV) for the security and safety of its staff and students.

2. Closed Circuit Television (CCTV) cameras are installed to view and record the activities of individuals overtly at selected locations on the School premises. The deployment of these cameras are a strategic component of the School's commitment to staff and student safety, security and crime prevention.

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

CCTV System

4. The CCTV system adopted includes internal / external; static colour / black and white; full pan, tilt and zoom cameras. Pan, tilt and zoom (PTZ) function is employed only on playback but not in real time live recording mode and area viewed is preset and static, especially for all external cameras.

5. The vast majority of CCTV cameras are IP based and connected to the School's IT network. The system records CCTV data in real time to specific Networked Video Recorders (NVR) in secure locations across the School estate.

6. Some CCTV cameras are set to motion detection, which means real time recording will be automated only when there are activities, that is, movement in the area. This ensures the system does not record when there are no activities taking place and guarantee sufficient disk recording space, maximise digital deletion or the recorded data ascribed retention period.

7. The member of staff responsible for the system is the Estates and Facilities Manager. The NFTS is the owner of all recorded CCTV data.

Purpose of the CCTV System

8. The purpose of the CCTV system is as follows:
   - To enhance safety, security and crime prevention on the School site
   - 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 the School and police in providing a swift response to criminal activity and provide evidential material for court and disciplinary proceedings.
- Protect the School's assets.
- To assist in traffic management within the School's car parks.
- To assist in supporting Health and Safety policies.
- To assist in the event of an emergency or disaster.

Scope

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

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

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

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

13. 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 the School.

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

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

Signage

16. Strategically placed CCTV camera notices at key entry points to the School's premises will advise individuals that they are entering an area which is covered by CCTV cameras.

17. The CCTV notice at entrances to the School and in adjacent areas will contain:
    - The name of the Data Controller (i.e. the NFTS)
    - The purpose(s) of the scheme
    - A contact name and telephone number for enquiries

Camera Locations

18. The CCTV systems installed in and around the School comprises 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.

19. Covert cameras are not installed anywhere on the School premises. However, the School 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 by the School's Director or law enforcement agencies.

Data Protection

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

21. 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.

22. The lawful basis identified for processing the personal data as part of the CCTV system is legitimate interests.

Responsibilities

23. The NFTS as owner has responsibility for compliance with the purposes and objectives of the system including operational guidance and the protection of the interests of the School users and privacy of the individuals whose images are captured on the system. This responsibility is undertaken by the following members of staff:

    - **The Data Protection Officer**- The Registrar 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 the School

    - **The Head of IT**- is responsible for protecting all data on the School's IT systems and will ensure there are appropriate technical and organisational security measures in place to protect CCTV data on the system

    - **The Estates and Facilities Manager**- shall have responsibility for the CCTV infrastructure, ensuring there is an adequate maintenance regime, upgrades to CCTV hardware and software, so they are fit for purpose. The Estates and Facilities Manager will develop and maintain good CCTV data processing and handling practice within the School in accordance with the Data Protection Policy and the Information Security Policy. The Estates and Facilities Manager is also responsible for the day to day management and control of the CCTV system on behalf of the School.

Access to CCTV Monitors and Monitoring Equipment

24. 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 images 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.

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

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

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

Recording and Storage of Information

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

29. The CCTV systems are operated and monitored 24 hours a day, every day of the year.

30. CCTV images not to be retained for longer than necessary. Data storage is automatically managed by the CCTV digital recorders which use software programme to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces a minimum of 45 days rotation in data retention.

31. Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal or disciplinary proceedings), the images will be erased following the expiration of the retention period.

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

33. Access to the CCTV System and to the captured images will be restricted to authorised staff involved in monitoring or investigation.

Access and Disclosure of CCTV Images

34. Requests for access to (review), or disclosure of (i.e. provision of a copy), of images recorded on the CCTV systems 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 have been recorded by the CCTV systems)
    - Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)

- Prosecution agencies (including School Managers in the course of Staff or Student disciplinary proceedings)
- Relevant legal representatives of data subjects

35. Images from CCTV must not be forwarded to the media for entertainment purposes or be placed on the internet.

36. Images will only be released to the media on the authority of the School's Director and following advice from law enforcement agencies to support police investigations.

Right of Access

37. Staff, students and other data subjects about whom the School holds or uses personal data have a legal right to access that information and 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@NFTS.co.uk

38. The School has discretion to refuse any third party request for information unless there is an overriding legal obligation such as a court order or information access rights. 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.

39. It may be necessary for redaction of images on copies of CCTV issued following a subject access request. This is usually to protect third party data. Where redaction is deemed impossible for example huge video files, the School may refuse a CCTV data request if providing this data infringes on the rights to privacy of others.

40. The contact point indicated on the CCTV signs around the School should be available to members of the public during normal business hours.

41. All disclosed CCTV data must be safely delivered to the intended recipient ideally by handing over information on a sealed data disc or other media storage device with encryption embedded in the CCTV application software. CCTV recorded data must not be transmitted by email.

42. Only the DPO and the Estates and Facilities Manager can authorise the viewing or release of CCTV data.

Liaison with Police Services

43. Images may be released to the Police Service or other law enforcement agencies in compliance with Police Act 1996 Section 30(1) and Section 29(3), Section 30(5) of the DPA 1998 now promulgated in the Data Protection Act 2018 and General Data Protection Regulations (GDPR 2018),

44. All CCTV data requests from the Police Services or other law enforcement agencies should be referred to the DPO.

45. Visiting police officers must provide their standard issued badge as proof of identity and provide signatures for any CCTV collected.

Installation

46. The CCTV installations are carried out through consultation with external CCTV providers approved by the NFTS.

47. 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.

48. The School 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.

Staff

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

50. Training will include how to identify suspicious behaviour, when to track individuals or groups and when to take close up views of incidents or people and compliance with Data Protection Act and any other relevant legislation. Staff with access to CCTV data should be particularly careful not to infringe upon the Public's Human Rights. The effectiveness of individual operators will be reviewed periodically**.**

51. Only authorised persons involved in the monitoring or investigation can view CCTV images.

52. The CCTV policy as with all other School 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.

53. Unless authorised by the DPO, only the Estates and Facilities Manager and their nominees may review stored recordings or down load information for the police or School

Complaints

54. All complaint and enquiries relating to the CCTV system should be addressed to: The Estates and Facilities Manager, NFTS, Station Road, Beaconsfield, HP9 1LG

Breaches of the Code

55. Breaches of the policy and of security will be investigated by the Estates and Facilities Manager or the Data Protection officer's nominee. Recommendations and corrective action plans will be put in place to remedy any breach which is proven.

56. The DPO is responsible for maintaining a record of CCTV data breaches as part of the policy.

57. All breaches of personal data must be reported to the DPO.

Updated June 2020