CCTV Policy

Introduction

This Policy aims to ensure that the scope, purpose and use of the CCTV systems installed and operated by Newcastle & Stafford Colleges Group College are clearly defined.

Scope

This Policy is binding on all members of Newcastle & Stafford Colleges Group and employees of contracted out services. It also applies to all other persons who maybe present, for whatever reason, on College property.

Principles

The following principles will govern the operation of the CCTV system:

• The CCTV system will be operated fairly and lawfully and only for the legitimate purposes as specifically authorised by the College.
• The CCTV system will be operated with due regard for privacy of the individual and in accordance with Article 8 of the European Convention on Human Rights i.e. an individual's right to privacy.
• The CCTV system is fundamentally an overt system, using non-hidden cameras within the confines of the College in public spaces.

Purpose of the CCTV system

The system is intended to provide an increased level of security for the benefit of those who study, work or visit the College. The CCTV system will be used to respond to the following legitimate aims / key objectives, which will be subject to annual review.

• To detect, prevent or reduce the incidence of crime.
• To prevent and respond effectively to all forms of harassment and public disorder.
• To improve communications and the operational response of staff in and around the areas where CCTV operates.
• To reduce the fear of crime.
• To create a safer community.
• To gather evidence by a fair and accountable method.
• To provide emergency services assistance.
• To assist with health and safety.
• To monitor the use of College car parking areas.

System details

The CCTV system comprises overt cameras situated on the College main and ancillary sites, displaying live video of the covered areas on screens and recording motion events on local storage (per building or camera).

Installation and signage

Cameras shall be installed in such a manner as not to intrude on private domestic areas. Cameras shall not be hidden from view and signs will be prominently displayed in the locality of the cameras. The signs will indicate:

- The presence of monitoring and recording.
- The ownership of the system.
- Contact telephone number.

If at any time mobile cameras are employed, their use will also be governed by this Policy.

Data Protection legislation

Where images of living, identifiable individuals are deliberately recorded, this creates personal data, the collection, use and storage of which is governed by data protection law in the UK (the General Data Protection Regulation and related EU and national legislation). Under data protection law, the College is identified as a data controller and as such is subject to a range of legal obligations when operating CCTV. Given that any particular sequence of CCTV recording may include personal data, all such recordings will be processed in accordance with the Data Protection Principles under the law, and Data Subject Rights, including the right of access to personal data, will be respected where recordings are confirmed to comprise personal data. These Data Protection Principles and Data Subject Rights are set out in full in Appendix 1. Where an individual requests access to recordings believed to include their personal data, the matter shall be referred to the Vice Principal.

Access to live footage and recordings

Access to Live Footage

Images captured by the system will be monitored by security staff. For operational purposes, and in accordance with the stated purposes of the system, only designated College staff trained in their duties and required to do so shall have access to live CCTV footage. Access to recordings is controlled and all staff are trained in their responsibilities in respect of the use of CCTV.

Access to Recordings

For operational purposes and in accordance with the stated purposes of the system, only designated staff shall have primary access to CCTV recordings. The Vice Principal or nominee must provide permission for the viewing of the CCTV recorded materials by specific College staff where this is

necessary in connection with the prevention of crime and anti-social behaviour, assisting in the apprehension and prosecution of offenders or matters of national security. Permission to disclose recordings will normally be granted in response to a legitimate request made by the Police in the course of their duties.

Disclosure of Recorded Material

As the main purpose of the CCTV system is to prevent crime and assist in the apprehension and prosecution of offenders, designated College staff may release CCTV recorded materials to the police where the College has initiated contact with the police and there is a reasonable belief that the CCTV recorded materials will be of assistance.

Where the police or other official body with prosecuting powers approach the College and request access to CCTV recorded materials they shall be asked to provide a Section 29 Notice (in the case of the police) or similar document confirming that the information is necessary for either the prevention of crime or the apprehension or prosecution of offenders, or matters of national security. Where any other person requests access to CCTV recorded materials, this request shall be forwarded to the Vice Principal.

In all cases where recorded materials are disclosed outside the College, the appropriate College staff shall ensure that the disclosure is logged and duly signed for.

A log will be kept recording all requests to the Vice Principal to review stored material. Note the log will not contain any personal data other than who requested and reviewed the material. The log can be made available on request for the purpose of establishing the frequency and purpose of requests made.

Retention of recorded materials and disposal

CCTV recordings and other materials produced from them shall be retained for no more than 30 days unless an incident is recorded which requires further investigation either by the College, the police or another external body with prosecuting powers.

In the case of an incident requiring further investigation recordings shall be kept for a maximum period of three years from the date of recording and in any event no longer than is necessary. All media, on which recordings were made, that are no longer required will be destroyed.

Breaches of the code and complaints

A copy of this Policy will be made available to anyone requesting it. Any complaint concerning misuse of the system will be treated seriously and investigated by the Vice Principal or nominee. Breaches of this Policy shall be dealt with in accordance with the appropriate disciplinary policy. Serious breaches of the Code may result in criminal liability on behalf of the individual which could be considered as gross misconduct.

Where appropriate, consideration will be given as to whether the police will be asked to investigate any matter relating to the CCTV system which may be deemed to be of a criminal nature.

Appendix 1

Data Protection Principles

The data protection principles state that personal data shall be:

• processed (i.e. collected, handled, stored, disclosed and destroyed) fairly, lawfully and transparently. As part of this, the College must have a 'legal basis' for processing an individual's personal data (most commonly, the processing is necessary for the College to operate a contract with them, the processing is necessary to fulfil a legal obligation, the processing is in the legitimate interests of the College and does not override their privacy considerations, or they have consented to the processing);

• processed only for specified, explicit and legitimate purposes;
• adequate, relevant and limited;
• accurate (and rectified if inaccurate);
• not kept for longer than necessary;
• processed securely.

Data Subject Rights

An individual's rights (all of which are qualified in different ways) are as follows:

• the right to be informed of how their personal data are being used. This right is usually fulfilled by the provision of 'privacy notices' (also known as 'data protection statements' or, especially in the context of websites, 'privacy policies') which set out how an organisation plans to use an individual's personal data, who it will be shared with, ways to complain, and so on;

• the right of access to their personal data;
• the right to have their inaccurate personal data rectified;
• the right to have their personal data erased (right to be forgotten);
• the right to restrict the processing of their personal data pending its verification or correction;
• the right to receive copies of their personal data in a machine-readable and commonly-used format (right to data portability);
• the right to object: to processing (including profiling) of their data that proceeds under particular legal bases; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest;
• the right not to be subject to a decision based solely on automated decision-making using their personal data.