# CCTV Policy

| | |
|---|---|
| Date Published | Mar 2019 |
| Next Review | Mar 2020 |
| UCC Governor Approval Committee | Resources Committee |
| UCC Staff Role Responsible | Site Manager / School Business Director |

*A copy of tis Statement of Intent should be signed and then displayed where it can easily be seen within the Reception area.*

# Closed Circuit Television (CCTV): Statement of Intent

Uppingham Community College takes its responsibility towards the safety of staff and pupils very seriously. To that end, we use Closed Circuit Television (CCTV) cameras to monitor the members of our school in a very specific way.

This policy must be used in conjunction with the school's Data Protection Policy.

The law states that we can use a CCTV system to monitor our premises, providing our system complies with the GDPR Data Protection Regulations.

The purpose of this policy is to:

- Manage and regulate the use of the CCTV system at Uppingham Community College.
- Show that we comply with the General Data Protection Regulations (GDPR).
- The images that are captured are useable for the purposes we require them for.
- Reassure those persons whose images are being captured.

This policy covers the use of CCTV and other systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Seeing what an individual is doing.
- Taking action relating to a crime.
- Using images of an individual in some way that could affect their privacy.

---

Signed by

_____ Head teacher _____ Date

_____ Chair of Governors _____ Date:

## UCC CCTV Policy 2019

### 1. Purpose of the CCTV system

The CCTV system in operation at Uppingham Community College will be used to:

- Maintain a safe environment by monitoring and recording restricted access areas at entrances to buildings and other areas
- Ensuring the welfare of students, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offense.

### 2. Compliance

### The Data Protection Act 2018 and GDPR

The Data Protection Act 2018 relates to data processing of all types. The definition of data under the Act is "Personal data" means any information relating to an identified or identifiable living individual. It requires the person to be identified by a number of means, which can include photographic or video footage.

The definition of Processing is much wider in its scope than the previous legislation ) "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as—
(a) collection, recording, organisation, structuring or storage,
(b) adaptation or alteration,
(c) retrieval, consultation or use,
(d) disclosure by transmission, dissemination or otherwise making available,
(e) alignment or combination, or
(f) restriction, erasure or destruction

Data in the case of CCTV recordings is in the form of recorded images of individuals that can be identified from these images.

Having regard for these definitions, it will be recognised that the use of CCTV for surveillance purposes is encompassed by the requirements of the Data Protection Act.

2.1. The CCTV system will be registered with the Information Commissioners' Office (ICO) under the terms of the GDPR 2018 .

2.2. The system will comply with all additional legislation including:

- The Commissioner's Code of Practice for CCTV 2008.
- The Surveillance Camera Code of Practice 2013, published by the Home Office.

## 3. Protocols

3.1. The CCTV system is a closed digital system which does not make audio recordings and has no wireless capability.

3.2. Warning signs will be placed at the entrances to the CCTV zone and further signs Placed inside the area.

3.3. The CCTV system has been designed for maximum effectiveness and efficiency. The college cannot however guarantee that every incident will be detected or covered and 'blind spots' may exist.

3.4. The CCTV system will not be trained on individuals unless an immediate response to an incident is required.

3.5. Additionally, the CCTV system will not be trained on private vehicles or property outside the perimeter of the school.

3.6. Recordings will only be released following written authority from the Police, or in respect of a subject access request.

3.7. The correct time and date is overlaid on the recorded image.

3.8. These date and time settings are checked and corrected as part of the routine maintenance visits

## 4. Security

4.1. Access to the CCTV system, software and data will be strictly limited to authorised operators and will be password protected.

4.2. The authorised CCTV system operators are:

- Mr Solly, Principal
- Mr G Swift, Network Manager
- Mr S Berridge, Site Manager
- Mrs K Croote, School Business Manager
- Mr A Cowling, Site Supervisor
- Mr J Rootham, Site Supervisor

4.3. The main CCTV control equipment is kept in a secure location which is locked when not in use. Visual display monitors are located in the Site Manager's Office and the ITS Office.

4.4. Camera systems will be properly maintained at all times.

## 5. Disclosure

5.1. The monitoring or viewing of images from areas where an individual would have an expectation of privacy is restricted to authorised personnel.

5.2. Disclosure of information from the CCTV systems will be controlled and consistent with the purpose(s) for which the system was established.

5.3. Images, both still and moving may be released to the police for the detection of crime under the terms of the GDPR .

5.4. Viewing of images by the police and subject access requests will be recorded in the event log.

5.5. Images will not be provided to third parties or bodies unless satisfactory documentary evidence is produced to show that they are required for legal proceedings, a subject access request, or in response to a Court Order.

## 6. Covert Recording

6.1. Fairness requires that we install signs to make individuals aware that they are entering an area where their images are recorded, it follows that failure to provide signs is a breach of the Data Protection Act.

6.2. However, we are able to rely on an exemption of the Data Protection Act which states that personal data processed for reasons of prevention and detection of crime and apprehension and prosecution of offenders are exempt. Providing that the following criteria are met:

a) We have assessed that if we had to inform individuals that recording was taking place it would prejudice our objective.

b) We have reasonable cause to suspect specific criminal activity is taking place.

c) That covert processing is only carried out for a limited and reasonable period of time and relates to the specific suspected criminal activity.

d) We have decided in principle that we wish to adopt covert recording. We have a clear documented procedure which sets out how we determine whether the use of covert recording is appropriate in an individual case. A confidential appendix regarding our decision that covert recording is appropriate is lodged with the Principal.

## 7. Subject access requests

7.1. Individuals whose information is recorded have a right to be provided with that information or, if they consent to it, view that information

7.2. When a request is received the information will be provided within 40 calendar days of receiving the request.

7.3. The College may charge a fee of up to £10 in such circumstances, which is deemed appropriate for subject access requests by the ICO.

7.4. Images will only be retained for as long as they are required. The system will automatically delete recordings after 31 days in accordance with GDPR.

## Appendix 1: Code of practice for the college website

A. Uppingham Community College operates a CCTV surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors.
B. The system is owned by the college and images from the system are strictly controlled and monitored by authorised personnel.
C. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the college and to ensure that its operation is consistent with the obligations on the college imposed by the GDPR The policy is available from the school's website.
D. The system will:
    - Always be for the purpose specified which is in pursuit of a legitimate aim.
    - Be designed to take into account its effect on individuals and their privacy and personal data.
    - Be transparent and include a contact point through which people can access information and complaints.
    - Have clear responsibility and accountability for images and information collected, held and used.
    - Have defined policies and procedures in place which are communicated throughout the school.
    - Only keep images and information for as long as required.
    - Restrict access to retained images and information with clear rules on who can gain access
    - Consider all operational, technical and competency standards relevant to a system and its purpose, and work to meet and maintain those standards in accordance with the law.
    - Be subject to stringent security measures to safeguard against unauthorised access and use.
    - Be regularly reviewed and audited to ensure that policies and standards are maintained.
    - Be used only for the purposes for which it is intended, including supporting public safety, protection of pupils and staff and law enforcement.
    - Be accurate and well maintained to ensure information is up-to-date.

## Appendix 2 - Incident Log

| Date of viewing | Persons viewing | Date of incident | Nature of Incident | Action Required | Signature |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Appendix 3

**The guiding principles of the Surveillance Camera Code of Practice**

| System operators should adopt the following 12 guiding principles: | Checked |
|---|---|
| Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need. | |
| The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified. | |
| There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints. | |
| There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used. | |
| Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them. | |
| No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged. | |
| Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes. | |
| Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards. | |
| Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. | |
| There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published. | |