



CARDINAL NEWMAN
CATHOLIC SCHOOL

October 2018

Date of Next Review:
October 2020

CCTV Policy

CARDINAL NEWMAN CATHOLIC SCHOOL & NEWMAN COLLEGE CCTV POLICY

Introduction

This policy must be read in conjunction with the detail on the Data Protection Registration Policy detailed on the school website.

The purpose of this policy is to regulate the management, operation and use of the CCTV system at Cardinal Newman Catholic School and Newman College (CNCS and NC)

Objectives of the CCTV Setup

- To increase personal safety of staff, students and visitors and reduce the fear of crime (Safeguarding arrangements).
- To protect the school buildings and their assets.
- To support the Police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect members of the public and private property.
- To assist in managing the school.

The system is a network based system and accordingly data is held in the school's server room. Cameras are installed at points of entry and exit into and out of the school. The cameras are also located on the outside of the school buildings with an overview of the school car parks.

Data Protection Act & CCTV Standards

Cardinal Newman Catholic School and Newman College (CNCS and NC) has chosen to use CCTV (Closed circuit television) in various areas across the school.

The Data Protection Act 1998, and Regulation of Investigatory Powers Act 2000 (RIPA) and CCTV Code of Practice issued by the Information Commissioner explains how CCTV systems should be used, so that schools and individuals can enjoy security and safety whilst ensuring that individual rights are upheld. CNCS complies with the Code and adopts good standards of practice which helps towards realising this objective. Use of CCTV can be affected by a number of Acts including the Data Protection Act, the Human Rights Act and the Regulation of Investigatory Powers Act (RIPA). Failure to comply with these Acts or the related codes would cause the school to be in breach of the Law, render any evidence as inadmissible or carry penalties for the school, as the CCTV user, or individual members of staff. Key staff have been provided with the necessary induction in the use of the CCTV systems and only those members of staff have access to the recordings within the system.

The school has undertaken the following checklist to ensure that the CCTV system remains within the law and that images can be used for crime prevention.

- The school has specified that the CCTV cameras have been installed for the safeguarding of staff and students and for detection and prevention of vandalism across the school estate.

- Significant signage is found in prominent positions in all areas where CCTV cameras operate to inform staff, students and the general public that they are entering an area where their images are being recorded either as still or video footage.
- The school retains the right to be the data controller for all footage recorded through the use of its CCTV cameras.
- The equipment is sited so that it only monitors those spaces that are intended to be covered by the equipment.
- All operators (staff who operate and monitor CCTV) are aware of the purposes for which the scheme has been established.
- Operators are aware that they are only able to use the equipment in order to achieve the purposes for which it has been installed i.e. safeguarding and the prevention and monitoring of vandalism.
- The images are stored in a secure server room and the retention period is for 4 weeks.

Management of the System & Code of Practice

The system is owned and operated by the school and is managed and supported by IT Tech Support. The system is installed onto a computer in the Tech Support Office.

Ordinarily, access to the system is restricted to IT Tech Support, the Principal and SLT. The footage may only be viewed by authorised members of staff.

Images required as evidence will be transferred to disk when required and stored in a secure location.

Breaches of the Code

- Any breach of the code of practice by the school will be initially investigated by the Principal, in order for them to take the appropriate disciplinary action.
- Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

Investigation & Reporting

Any member of the school community i.e. staff member or student may identify a security threat to the school. This potential incident should be reported to the Principal or another designated member of the Senior Leadership team.

The SLT member will request that data be researched on the system, providing as much detailed information as possible e.g. incident occurred between 9.00 a.m. and 9.30 a.m. in the Cashman building, ground floor corridor.

IT Tech Support will access the system and download the information required. This will be completed in a secure environment and the information will remain confidential.

In the event that the system identifies 'unacceptable or inappropriate' behaviour, the school's procedures for such incidents will be followed (Behaviour Policy, Sanctions, Discipline procedures etc.)