Cumran Primary School
CCTV Policy

Version	Date	Revision Author	Summary of Changes
1.0	April 2024	R Moles/ P McDade	

EXECUTIVE STATEMENT

At Cumran Primary School, we believe privacy is important. We are committed to complying with our data protection obligations and to being concise, clear and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

This Policy is intended to reflect the school's implementation of CCTV through following best practice advice from the Information Commissioner's Office (ICO). We will review and update this CCTV Policy regularly in accordance with our data protection obligations.

Any queries in relation to this Policy or any of the matters referred to in it should be submitted to the Principal/ Vice-Principal by contacting the school by telephone (028 44811352) or by email info@cumran.clough.ni.sch.uk

The following policies, procedures and documents are also relevant to this Policy:

- School Data Protection Policy
- Subject Access Request Procedure
- Department of Education Model Disposal of Records Schedule for Schools

Other relevant policies may be accessed on the school website

https://www.cumranprimary.co.uk/policies/

1. Introduction

1.1 Cumran Primary School has CCTV surveillance in place. We use CCTV cameras to view and record individuals on and around our premises in order to maintain a safe environment for our pupils, staff and visitors. However, we recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with Data Protection Act 2018 and the UK GDPR.

1.2 CCTV systems are installed on the school premises; therefore, this Policy applies to teaching staff, non-teaching staff, volunteers, pupils, parents/carers, contractors and other visitors to the school, including members of the public.

1.3 The purpose of this Policy is to:

a) set out why and how we will use CCTV, and how we will process data recorded by CCTV cameras

b) ensure that the legal rights of data subjects, relating to their personal data, are recognized and respected

c) assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence

d) explain how to make a subject access request in respect of personal data created by CCTV.

2. Purpose of CCTV

2.1 The School has identified a need for CCTV externally**.** We have outlined below the reason(s) we use CCTV around our site:

(a) To reduce the fear of crime: Individuals work on their own in the building for significant parts of the day, and frequently the building is locked up at night by individuals. The presence of CCTV will provide a degree of assurance to individuals that the personal risk is reduced.

(b) To deter and prevent crime eg: instances of anti-social behaviour, individuals being abusive and, or refusing to leave the premises when requested to do so, or attempting to enter the premises when events are taking place or when the School is closed. It is intended that CCTV will act as a deterrent.

(c) To protect property: The presence of CCTV is intended to reduce crime, including vandalism to the School buildings/infrastructure and parked vehicles, theft of School and personal property from the building and vehicles, and graffiti on exterior walls.

(d) Provide assistance in the detection of crime: in the event that any criminal incidents of any kind do occur, to provide high quality evidence which may

assist in identifying individuals involved and where appropriate detecting crime and apprehension and prosecution of offenders.

(e) To improve and provide assistance with issues relating to the health and safety of pupils, staff and visitors: it is intended that in the event of any incident which may raise Health and Safety concerns, which CCTV may assist in determining the cause of the incident and any measures which need to be taken as a result of incidents.

(f) *To assist in child protection by deterring inappropriate behaviour and providing assurances to staff, volunteers and parents that evidence from CCTV may be available should the need arise to investigate an alleged or actual Child Protection incident.*

*This list is not exhaustive and other purposes may be or become relevant.

3. Who is Responsible for this Policy

3.1 For the purpose of the Data Protection Act 2018 and the UK GDPR, the School is the Data Controller of the CCTV surveillance system. The School's ICO Registration number is: Z7954223

3.2 The School Board of Governors and Principal/Vice-Principal have overall responsibility for the effective operation of this policy. The Principal/Vice Principal are the primary contact for the day-to-day application of this policy therefore any questions in relation to this policy should be referred to the Principal/Vice-Principal in the first instance.

3.3 This Policy will be reviewed annually by the School Board of Governors and Principal/Vice Principal, who may also consult with the School's DPO, if appropriate. The school will also review the ongoing use of existing CCTV cameras in the school, annually, to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction in line with all relevant ICO guidance and seek to comply with its best practice suggestions.

3.4 Any and all future changes to CCTV systems or the addition of CCTV systems (or other surveillance systems) will be subject to the completion of a satisfactory Data Protection Impact Assessment (DPIA).

4. CCTV System Overview

4.1 The School's CCTV system is capable of recording **24 hours per day, 7 days per week.** Images will be recorded and retained on a 30 day rolling period, unless the School is required by law to retain them and/or it is necessary for the school to retain any footage as part of the investigation of an incident. In the case of the latter the relevant footage will be stored securely until it is no longer required for the purpose for which it was retained. Otherwise, the CCTV System will automatically delete the images it records after 30 days.

4.2 If a third party notifies the School that it intends to seek a court order for production of CCTV footage held by the school, the School will delete the footage after 12 months if it has not received a court order for production during that period (and will inform the relevant third party of its intention to do so).

4.3 The CCTV system monitors the external areas of the school such as play areas and the carparks, entrances and exits. It will exclude internal public areas eg: corridors, foyers, large rooms used for public gatherings, assembly or sports halls.

4.4 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. CCTV cameras will only cover school buildings/premises (external), car parks and public areas on the school site ie: front entrance to the school, the staff car park to cover the main vehicle entrance, the back of the canteen looking out onto the small playground, the junior playground and senior playground.

4.5 CCTV will not cover external public areas other than paths and roads immediately beside the school premises, which will be limited to the degree possible by positioning and technical controls. CCTV cameras will also be positioned to avoid all neighbouring premises.

4.6 CCTV operating staff will be limited to a small number of individuals appointed by the Board of Governors, who will be required to be conversant with the School's CCTV Policy and Data Protection Policy when appointed. CCTV Operating Staff will also be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data. Access to recorded images will be strictly controlled and only available under conditions set down by the Board of Governors.

4.7 In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure the Network based CCTV recorder on premises will be operated in a locked room with restricted access, and with password protection on the system to limit access to only approved personnel.

4.8 In order to inform people that they are under surveillance we will display clear CCTV signage appropriately around the School premises in the locations wherein CCTV cameras have been positioned. The signage will be easy to read, well-lit and positioned in places where they can be easily seen by individuals. Signage displayed will give details of someone in the school that can provide further advice under guidance in relation to any data protection queries. Privacy notices, Data Protection and CCTV policies are available on the school website.

4.9 The School CCTV systems audio recording will be disabled as this is may be considered intrusive and unnecessary in most circumstances and could thereby undermine support and confidence. Nor do the School CCTV systems have the ability for facial recognition. The CCTV recorder on the premises will be operated in a locked room with restricted access, and with password protection on the system to limit access to only approved personnel.

5. Requests for Disclosure

5.1 To Individuals

5.1.1 Any request for images by an individual data subject which relate to themselves or a third party acting on their behalf, i.e. "*Subject Access Requests*" should be made directly to the School, marked for the attention of the School Principal. Such requests will be processed in line with Data Protection Legislation and the school's Subject Access Procedure. Identification and/or a sufficient 'form of authority' will be sought by the school upon receipt of such a request.

5.1.2 In order for the school to locate the relevant images sufficient detail should be provided by the requester, such as date/location and time. The method of disclosure will be determined based on the nature and source of the request received. Where appropriate, disclosure will be on site visiting/ viewing but, where it is necessary to release copies of footage, this will be done securely using encrypted digital media.

5.1.3 Where images include third parties, the school may not be in a position to release the image/footage where doing so would place them in breach of Data Protection Legislation. Requests will be processed on a case by case basis and the 'right of access' granted when appropriate. Any disclosure of CCTV footage will be in compliance with the schools internal processes which are fully compliant with UK GDPR and the Data Protection Act 2018, specifically our Data Protection Policy and our CCTV policy.

5.2 To Third Parties

5.2.1. CCTV footage will not be routinely shared with external agencies or bodies, whether statutory prosecution agencies, the judicial system, local government agencies, legal representatives, data subjects or other external bodies except upon receipt of a valid request. For example, it may be necessary for us to share recorded footage in limited circumstances such as where a law enforcement agency is investigating a crime. These images may be disclosed via viewing or by providing a copy of the images.

5.2.2 The School will consider all such requests in line with Data Protection Legislation and release images only where a relevant exemption to the Data Protection Legislation applies. School will adhere to procedure and statutory obligations in respect of right of access.

6 Complaints

6.1 Any complaint regarding the School's CCTV will be dealt with in line with the School's Complaints Policy, which is available at

https://www.cumranprimary.co.uk/policies/

6.2 You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The ICO's contact details are as follows:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01 625 54 57 45/0303 123 1113, website: www.ico.org.uk

Definitions

For the purposes of this policy, the following terms have the following meanings:

CCTV: means fixed cameras designed to capture and record images of individuals and property.

Data: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data subjects: means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

Data controllers: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law.

Data users: are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

Data processors: are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Processing: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.