The Rivers
C.of E. Academy Trust

CCTV Policy

Burlish Park Primary School

This document sets out the regulations for the MAT and all member academies

Contents

Introduction 2
Definitions 2
Reasons for the use of CCTV 2
Monitoring 3
How we will operate any CCTV 3
Use of data gathered by CCTV 3
Retention and erasure of data gathered by CCTV 4
Use of additional surveillance systems 4
Requests for disclosure 4
Subject Access Requests 5
Complaints 5
Data protection right 5

Introduction

This policy is intended to clearly set out the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) which are relevant to Trust use of CCTV and video surveillance.

This policy applies to all of our workforce including employees, trustees, governors, consultants, self-employed contractors, casual workers, agency workers and volunteers. It also applies to anyone visiting our premises.

A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

Definitions

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

- CCTV means fixed and domed cameras designed to capture and record images of individuals and property.
- Data processor means any person or organisation that is not part of our workforce that processes personal data on our behalf and on our instructions.
- 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.
- Process, processing or processed means any operation performed on personal data. This includes collecting, recording, organising, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available or destroying personal data.
- 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 video surveillance technology that may be introduced in the future that capture information of identifiable individuals or information relating to identifiable individuals.
- Workforce means any individual employed by Trust such as staff and those who volunteer in any capacity including advocates, Trustees / Members/ parent helpers.

Reasons for the use of CCTV

We currently use CCTV around our premises as set out below. The use of CCTV is necessary for legitimate purposes including:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime.
- for the personal safety of staff, pupils, visitors and other members of the public and to act as a deterrent against crime.
- to support law enforcement bodies in the prevention, detection and prosecution of crime.

- to assist in day-to-day management of the School, including ensuring the health and safety of staff, pupils and others.
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.
- to assist in the defence of any civil litigation, including employment tribunal proceedings.
- to assist in the effective resolution of complaints which arise.

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

Monitoring

CCTV monitors the exterior of our premises and playgrounds, 24 hours a day and this data is continuously recorded.

Camera locations are chosen to minimise viewing spaces not relevant to the legitimate purposes of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

Images are monitored by authorised members of staff at various times during the day. Staff using surveillance systems will be given appropriate training to ensure that they understand and observe the legal requirements related to the processing of relevant data.

How we will operate any CCTV

Where CCTV cameras are placed on our premises, we will ensure that signs are displayed at the entrance of the surveillance area to alert individuals that their image may be recorded. The signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices.

Use of data gathered by CCTV

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

Given the large amount of data generated by surveillance systems, we may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

Retention and erasure of data gathered by CCTV

Data recorded by the CCTV system will be stored digitally. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. In all other cases, recorded images will be kept for no longer than 25 days.

At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

Use of additional surveillance systems

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location or location where pupils are likely to be recorded, we will carefully consider if they are appropriate by carrying out a data protection impact assessment (DPIA).

A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

Requests for disclosure

No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Data Protection Officer. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

We will maintain a record of all disclosures of CCTV footage.

No images from CCTV will ever be posted online or disclosed to the media.

Subject Access Requests

Individuals may make a request for disclosure of their personal data, and this may include CCTV images (data subject access request). A data subject access request for any CCTV footage should be directed to the Data Protection Officer.

In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

We reserve the right to obscure images of third parties when disclosing CCTV data as part of a data subject access request, where we consider it necessary to do so. Where the circumstances of an incident mean that it is not possible to effectively obscure images of third parties, we reserve the right to refuse the request on the basis that it would reveal the identities of third parties.

Complaints

If any individual has any concerns about our use of CCTV, they should speak to the Data Protection Officer in the first instance.

Where this is not appropriate, or matters cannot be resolved informally, our workforce should use our formal grievance procedure. Any other individuals should make a complaint in accordance with our Data Protection Policy.

Data protection right

We recognise that, in rare circumstances, individuals may have a legal right to request erasure of personal data concerning them or to restrict the processing of their personal data. Any individual who considers that these rights apply to them in relation to our use of CCTV should speak to the Data Protection Officer in the first instance.