



DOLLAR ACADEMY

CCTV POLICY STATEMENT

At Dollar Academy, we believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, pupils, and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by surveillance systems are personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, relating to their personal data, are recognised and respected.

In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence. This policy is intended to assist our staff, pupils, parents/guardians, and visitors in understanding how we may use CCTV for the purposes of maintaining a safe and secure environment.

This CCTV Policy was prepared with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of our CCTV activities and how they may relate to our handling of your personal information. However, we are happy to provide additional information or explanation needed.

If you have any questions, comments or requests regarding our CCTV Policy then please do not hesitate to get in touch with us. To make things easier for both of us we would appreciate it if your queries were addressed to:

Mr Robin Macpherson
Assistant Rector
Dollar Academy
Dollar
FK14 7DU

Macpherson-r@dollaracademy.org.uk

or

Telephone: 01259 742511

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: means 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 such as staff, parents/guardians, and pupils.

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 other data protection policies.

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 body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

ABOUT THIS POLICY

We currently use CCTV cameras to view and record individuals on and around premises owned or managed by the school. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

We recognise that information that we hold about individuals is subject to the General Data Protection Regulation (“**GDPR**”) (EU) 2016/679 plus any other data protection laws that may amend, vary, or replace the GDPR (together “**Data Protection Legislation**”).

We are committed to complying with all our legal obligations under Data Protection Legislation. The images of individuals recorded by CCTV cameras at the school are personal data and therefore subject to the Data Protection Legislation.

We are a data controller and we have registered our use of CCTV with the Information Commissioner. We also seek to comply with best practice suggestions from the Information Commissioner's Office (the "ICO").

This policy covers all employees, pupils, parents/guardians, directors, officers, consultants, contractors, freelancers, volunteers, interns, casual workers, and may also be relevant to visiting members of the public.

This policy is non-contractual and does not form part of the terms and conditions of any other contract. We may amend this policy at any time. The policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

The Board of Governors of the School has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to Mr Robin Macpherson, Assistant Rector. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of Mr David Yuill-Kirkwood.

REASON FOR THE USE OF CCTV

We currently use CCTV in and around the School as outlined below. We believe that such use is necessary for legitimate purposes, including:

1. To prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
2. For the personal safety of staff, pupils, parents/guardians, visitors and other members of the public when visiting or attending the School and to act as a deterrent against crime;
3. To support law enforcement bodies in the prevention, detection and prosecution of crime;
4. To assist in day-to-day management, including ensuring the health and safety of staff, pupils, and others; and
5. To assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.

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

We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed every twelve months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

MONITORING

Our CCTV monitors the exterior of the School buildings, including both the main entrance and secondary exits.

Our CCTV system operates twenty-four hours a day and this data is continuously recorded.

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

Images may be monitored by authorised personnel 24 hours a day, every day of the year.

No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Rector or the Bursar. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced or unless the School decides it is needed in order to resolve a dispute or grievance or disciplinary situation involving a pupil or parent or member of staff.

In other appropriate circumstances, we may allow law enforcement agencies or legal advisors 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.

Images from CCTV will not normally be posted online or disclosed to the media.

HOW WE OPERATE CCTV

Live feeds from CCTV cameras will only be **continuously** monitored where this is reasonably necessary, for example to protect health and safety.

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 or senior teaching staff involved with disciplinary or grievance matters. Recorded images will **usually** only be viewed in 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. The video footage will be stored on a cloud computing system within the European Economic Area only and we will not transfer data outside of the European Economic Area.

RETENTION AND ERASURE OF DATA GATHERED BY CCTV

Data recorded by the CCTV system will be stored digitally within the school. It is automatically securely dated and time stamped. 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 or are needed, in line with our privacy notice and data retention policy. 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 most other cases, recorded images will be kept for no longer than 90 days. Some cameras auto-delete on a regular basis.

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 or School location, we will carefully consider if they are appropriate by carrying out a data privacy 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.

COVERT MONITORING

We will **only rarely** engage in systematic covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place); **for example** when there are reasonable grounds to suspect that criminal activity or extremely serious misbehaviour is taking place and, after suitable consideration, we reasonably believe that **this is the best way to tackle the issue**.

In the event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Rector or Bursar with the agreement of the Chair of the Board of Governors. The risk of intrusion on innocent staff, pupils, and visitors will always be a consideration in reaching any such decision.

Only limited numbers of people will be involved in any covert monitoring.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

SUBJECT ACCESS REQUESTS

Data subjects may make a request for disclosure of their personal information and this may include CCTV images (data subject access request). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, and you can find our contact details at the top of this CCTV Policy.

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.

As a result of Data Protection Legislation it may be necessary to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

COMPLAINTS

If any member of staff, a pupil, parent/guardian, or member of the public who reasonably believes they may have been captured by our CCTV camera, has questions about this policy or any concerns about our use of CCTV, then they should contact the School using the contact details at the top of this CCTV Policy.

If you are not satisfied with the way that we have handled any of your requests or queries relating to our use of your personal data then you can contact the ICO at www.ico.org.uk. The Information Commissioner's Office is the statutory body responsible for overseeing data protection legislation and law in the United Kingdom.

REQUESTS TO PREVENT PROCESSING

We recognise that, in rare circumstances, individuals may have a legal right to prevent processing likely to cause substantial and unwarranted damage, or to prevent automated decision making. For further information regarding this, please contact us using the details provided at the top of this CCTV Policy.

Publication and Review:

Date published: February 25th, 2019

Review date: February 25th 2020

Reviewer: Mr Robin Macpherson, Assistant Rector