

Charles Darwin School

(Part of the Charles Darwin Academy Trust)

Policy Document

|  |  |
| --- | --- |
|  Policy Name | Closed Circuit Television (CCTV) Policy and Code of Practice |
|  Approved by:  | CDAT Board – 13th July 2018 |
|  |  |
|  |  |
|  SLT Responsible: | Head teacher – Aston Smith |
|  Other staff:Authorised staff: | ICT Manager Naj Naseer – Responsible OfficerICT Assistant Luke D’Andrea – System User |
| Appendices | Librarian Susan Adams – System User |

Contents

[1. Introduction 3](#_Toc481489437)

[2. Objectives of the CCTV System 4](#_Toc481489438)

[3. Responsibility 4](#_Toc481489439)

[4. Statement of Intent 5](#_Toc481489440)

[5. Operation of the System 5](#_Toc481489441)

[6. Purchase and Deployment of CCTV Cameras 5](#_Toc481489442)

[7. Control of Software and Access to the System 6](#_Toc481489443)

[8. Monitoring/Live Viewing Procedures 6](#_Toc481489444)

[9. Signage 6](#_Toc481489445)

[10. Breaches of the Code (including breaches of security) 7](#_Toc481489446)

[11. Complaints 7](#_Toc481489447)

[12. Subject Access and Freedom of Information 7](#_Toc481489448)

[13. Recordings and Disclosure Procedures 8](#_Toc481489449)

[14. Hard Copy Prints 9](#_Toc481489450)

**Charles Darwin School**

**(Part of the Charles Darwin Academy Trust)**

Closed Circuit Television (CCTV) Policy and Code of Practice

# Introduction

Charles Darwin School (the ‘School’) has a comprehensive Closed Circuit Television (CCTV) system (‘the 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.

The System is owned by the School and data from the System is strictly controlled and monitored by authorised personnel only.

In addition to School policies, procedures, and guidelines, this Policy has been prepared with support from the standards set out in:

* The Data Protection Act 1998 (DPA) (Until May 25th 2018)
* The General Data Protection Regulation (GDPR) (From May 25th 2018)
* The Freedom of Information Act 2000 (FOIA)
* The Protection of Freedoms Act 2012
* The Home Office Surveillance Camera Code of Practice June 2013

In line with the Surveillance Camera Commissioner 12 guiding principles, the use of the System will:

* Always be in accordance with its specified purpose, which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
* Take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
* Have as much transparency as much as possible, including a published contact point for access to information and complaints.
* Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used.
* Have clear rules, policies and procedures in place, which will be communicated to all who need to comply with them.
* Store images and information for no longer than strictly required for the stated purpose of the System, and such images and information will be deleted once their purposes have been fulfilled.
* Restrict access to retained images and information and have 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.
* Consider any approved operational, technical and competency standards relevant to a System and its purpose and work to meet and maintain those standards.
* Be subject to appropriate security measures to safeguard against unauthorised access and use to data.
* Have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice.
* Be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value when the use is in pursuit of a legitimate aim, and there is a pressing need for its use.
* Be accurate and kept up to date when any information used to support a surveillance camera System which compares against a reference database for matching purposes.

# Objectives of the CCTV System

The primary purpose of the System is to:

* Protect the school buildings and their assets
* Increase personal safety and reduce the fear of crime
* Support the Police in a bid to deter and detect crime
* Assist in identifying, apprehending and prosecuting offenders
* Provide evidence for the school to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, pupils or other visitors on the site that breaches or is alleged to breach the school’s policies
* Protect members of the school community, public and private property
* Assist in managing the school

Additionally, each camera installation may have its own additional task specific objectives, which will be defined during the Installation Consideration phase and evaluated against during subsequent Reviews.

The System will not be used for any other purpose other than those set out in this policy document and supporting Installation Consideration and Review documents without prior consultation.

The Head teacher is responsible for the operation of the System and for ensuring compliance with this policy. The Head teacher will be supported in this role by the ICT Manager.

The System will not be used to monitor the progress of staff, students or other individuals in the ordinary course of lawful business in the area under surveillance. Nor are managers permitted to use the System to observe staff working practices or time keeping or to assist them in the day-to-day management of their staff.

Individuals will only be specifically monitored if there is reasonable cause to suspect a criminal offence or serious breach of discipline, potentially amounting to misconduct has been, or may be, about to be committed and this will only be permitted when authorised. Consultation with the Head teacher will be made before any such action is taken.

# Responsibility

**Head teacher**

The Head teacher has overall responsibility for the System.

**Responsible Officer**

The day-to-day operational responsibility rests with the designated Responsible Officer and their staff who actually operate the CCTV equipment and handle the data. They will:

* Make sure that authorised staff using the System are properly trained in the use of the equipment and comply with the Code of Practice, policies and procedures. They are not to permit any other staff to operate the equipment or view images without authorisation.
* Act as the first point of contact for enquires and requests for evidence and as the liaison officer for all external and internal contacts.
* Review all CCTV documentation relating to the System annually (or as changes occur) and ensure the information in those documents is up to date

**Staff Operating the System (System User)**

Staff operating the System are responsible for:

* Operating the equipment in accordance with requirements set out in current legislation, this policy document, guidelines, confidentiality certificates, Codes of Practice and local Operational Manuals.
* Ensuring that their training is up to date.
* Bringing any faults or misuse of the equipment to the Responsible Officer’s attention immediately.

**Data Controller**

For the purposes of the Data Protection Act 1998/General Data Protection Regulation (GDPR), the Data Controller is Charles Darwin School and the School is legally responsible for the management and maintenance of the CCTV system.

# Statement of Intent

The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998/General Data Protection Regulation (GDPR) and the School will seek to comply with the requirements both of the Data Protection Act/General Data Protection Regulation (GDPR) and the Commissioner's Code of Practice, as well as the Surveillance Camera Code of Practice 2013 published by the Home Office.

The School will treat as data all CCTV recordings and relevant information.

The System will be used to monitor activities within the School and its grounds in line with the objectives of the scheme.

Materials or knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purpose, or for the purpose of entertainment. Recordings will only be released under the written authority from the Police, or in respect of a subject access request.

The School has endeavoured to ensure that the planning and design of the scheme will give maximum effectiveness and efficiency. It is not possible, however, to guarantee that the System will cover or detect every single incident taking place in the areas of coverage.

# Operation of the System

The System will be administered by the Responsible Officer and relevant System Users in accordance with the principles and objectives expressed in this Policy.

The System will be in operation 24 hours each day, for every day of the year.

The Responsible Officer will check on a weekly basis that the System is operating effectively and in particular that the equipment is properly recording and that cameras are functional. The System will be regularly serviced and maintained, and defects will be rectified at the earliest convenient opportunity.

Recording equipment and recording media will be kept in a secure location and no access will be granted to unauthorised staff.

# Purchase and Deployment of CCTV Cameras

Charles Darwin School is committed to respecting people’s rights to privacy and supports the individual’s entitlement to go about their lawful business. This is a primary consideration in the operation the System, although there will inevitably be some loss of privacy when CCTV cameras are installed.

Serious consideration will be given to the necessity for cameras in a given location, and their impact on the privacy of individuals using the areas where cameras are to be installed.

The School will not use CCTV cameras if there are cheaper, less intrusive and more effective methods of dealing with the problem.

If after looking at all the alternatives it is decided that CCTV is the only suitable solution a clear operational objective for the System and each camera must be identified and an assessment on the impact on privacy must be carried out. A record of these decisions must be retained for inspection and review every year.

It is a requirement under the Information Commissioners Code of Practice that any equipment purchased is fit for purpose and will meet the objectives set down for the scheme. There is also a clear requirement for all CCTV schemes to have an effective maintenance schedule and Code of Practice.

Covert cameras are not normally to be deployed into areas used by staff, students or the public. Cameras should normally be clearly visible and clearly signed.

The School will not purchase cameras that can monitor conversation or be used to talk to individuals as this is seen as an unnecessary invasion of privacy.

# Control of Software and Access to the System

Access to the CCTV software will be strictly limited to authorised operators (System Users) with a password, and physical access to the relevant rooms secure.

System Users must satisfy themselves that all persons viewing CCTV material will have a right to do so, and disclosure requests will be undertaken in accordance to this Policy.

Other administrative functions will include controlling and maintaining downloaded digital materials, and maintenance and system access logs.

# Monitoring/Live Viewing Procedures

Camera surveillance may be maintained at all times.

A monitor is installed in the School’s IT Technical office and library. Access to monitors is restricted to staff where those areas being monitored are not in plain view.

Monitoring of other cameras will only be carried out by persons authorised by the Responsible Officer to meet the intended purpose of the camera installation.

# Signage

Visitors and the general public are made aware of the presence of the System and its ownership by appropriate signage and the publication of this policy on the School’s website.

All areas where CCTV is in use are clearly signed to comply with the Data Protection Act/General Data Protection Regulation (GDPR).This is to warn people that they are about to enter an area covered by CCTV cameras or to remind them that they are still in an area covered by CCTV. The signs will also act as an additional deterrent. CCTV signs should not be displayed in areas which do not have CCTV cameras.

The signs should have a yellow background with all writing in clear black print. The signs should carry the CCTV camera and Charles Darwin School Logo. The information on the sign should explain why the CCTV cameras are there, who runs them, and contact details. The signs, position and the message needs to be big enough to enable people to easily read the information on it.

# Breaches of the Code (including breaches of security)

Breaches of the policy by staff monitoring the System may constitute matters of discipline under the relevant conditions of employment.

Any breach of the CCTV Code of Practice by school staff will be investigated by the Head teacher, in order for him/her to take any appropriate disciplinary action

# Complaints

It is recognised that other members of the School may have concerns or complaints in respect of the operation of the System. Any concerns or complaints in respect of the System’s use or regarding compliance with this policy should be addressed to the Head teacher.

# Subject Access and Freedom of Information

All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of Data Subject (that is, the person whose image has been captured by the CCTV system) access requests.

Data Subjects will be asked to put in writing any requests for access. A form is available upon request for use if the Data Subject wishes to do so. However, any formal request in writing, including via email, fax, or social media, will be accepted. Individuals should provide:

* Dates and times when they visited the School and their location; for example, which specific area or building
* If the request is considered to be either ‘manifestly unfounded or excessive’, or if the individual requests further copies, then the school may elect to charge a fee to cover administrative costs. Either a cheque or cash to the required sum should be provided to the school. The fee will be as reasonable as possible and where possible, will total £10.00 for which a receipt will be issued.

The Data Subject will be asked whether they would be satisfied with merely viewing the images recorded.

The Data Subject may be asked to provide further information in order for the school to verify their identity.

If a fee is to be charged then the school will not comply with a request until the fee has been received, and the School will contact the Data Subject promptly and inform them that they need to pay.

A written decision on their request will be sent to the Data Subject within 21 days and, if access to the images is to be provided (see below for circumstances when it may be refused), such access will usually be provided within one month from the day after the request is received. If the data subject has been asked to provide further information to verify their identity, then the period for response will begin once the information has been provided. If the request is complex or if the volume of data requested is too great to process within the first month then a further two months extension may be applied. The Data Subject will be notified within 21 days and the reason for the extension explained if an extension must occur.

The procedure outlined above and the use of the Subject Access Request form complies with Article 15 of the General Data Protection Regulation (GDPR), enabling the Head teacher to inform individuals as to whether or not images have been processed by the CCTV system and whether or not the school will comply with a Subject Access Request.

The School is not obliged to comply with a request under this section unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the information which that person seeks.

The school may refuse to comply with the request if it is considered to be ‘manifestly unfounded’, excessive or repetitive in nature.

# Recordings and Disclosure Procedures

Persons other than those specified,the police, or the Data Subject may be authorised to access the CCTV material on a case-by-case basis.

Written authorisation is required and access to recorded images in these circumstances will only be granted where it is consistent with the obligations placed on the School by the Data Protection Act 1998 (DPA) /General Data Protection Regulation (GDPR).

Each separate visit will require individual authorisation and will be supervised at all times. Persons will not be given access to any data which falls within the scope of the Act.

All requests for access or disclosure will be recorded, and if access or disclosure is denied, the reasons will be documented.

If access to or disclosure of the CCTV material is allowed then the following will be documented:

* The date and time at which access was allowed or the date on which disclosure was made
* The reason for allowing access or disclosure
* The extent of the information to which access was allowed or which was disclosed

The Responsible Officer will make decisions on access to recorded images by persons other than police officers. Requests by the police for access to images will not normally be denied and can be made without the above authority, provided they are accompanied by a written request signed by a police officer who must indicate that the images are required for the purposes of a specific crime enquiry.

In an emergency, and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to access the System.

Recorded images will only be reviewed with the authority of the Responsible Officer.

It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the procedures.

Copies of digital images will only be made for the purposes of crime detection, evidence in relation to matters affecting safety, evidence in relation to matters of breaches to the School’s policies, evidence for prosecutions, or where otherwise required by law.

All staff involved in the operation of the System will, by training and access to this policy, be made aware of the sensitivity of handling CCTV images and recordings.

As the images are recorded digitally, the process of identifying retrieval dates and times will be computerised. Images will be cleared automatically after a set time, which, unless required for evidential purposes or the investigation of crime, is no longer than 60 days from the date of recording. However, the School recognises that, in accordance with the requirements of the Data Protection Act / General Data Protection Regulation (GDPR), no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images.

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images.

These aspects of the policy reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998 and the key principals outlined in Section 5 of the General Data Protection Regulation (GDPR).

All staff should be aware of the restrictions set out in this policy in relation to access to, and disclosure of, recorded images.

Appropriate forms will be used to document routine disclosure to the Police.

# Hard Copy Prints

Hard copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected and will be treated in the same way as digital images.

At the end of their useful life all computer disks, still photographs and hard copy prints will be disposed of as confidential waste.

**Document Control**

|  |  |  |
| --- | --- | --- |
| Date modified | Description of modification | Modified by |
| 22.5.2018 | Amendments to include GDPR legislation | RBL |