Use of the CCTV System Policy

This service is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment

Governor's Committee Responsibility:	Resources
Date Approved:	Spring 2020
Review Period:	Annually
Next Review Date:	November 2021

Produced by LM October 2020, reviewed by GC November 2020

Introduction

The purpose of this policy is to regulate the management, operation and use of the closed-circuit television (CCTV) at Jersey Music Service. This policy follows the guidelines published in the Data Protection Law (Jersey) 2018 on the use of CCTV in public places.

The system

Camera positions have been carefully located to ensure they are appropriate and effective whilst minimising any collateral intrusion. It is impossible, however, to ensure that every incident will be seen and recorded. The CCTV system will be maintained in accordance with the Data Commissioners CCTV code of practice guidelines (2008) and this policy.

Maintenance checks

- Cameras will be checked once a week to ensure that they are operational.
- The recorder will be checked once a month to ensure it is recording and it is possible to download images.
- Camera fixings will be checked to ensure safety and security during planned maintenance e.g. cleaning cameras.
- Repairs will be made to the system within two weeks if practical, dependent upon cost and CCTV review.

Camera images will be recorded and displayed on a CCTV monitor in the Business Manager's Office. The recording media is a DVR recorder; images are stored on a hard drive which is automatically overwritten after thirty days. Viewing monitors are also available in the Administration Office.

Purpose of CCTV

It shall be used for the purpose of:

- Increasing the personal safety of staff, students and visitors and reduce the fear of crime.
- Protecting the service buildings and their assets.
- Supporting the Police in a bid to deter and detect crime.
- Assisting in identifying, apprehending and prosecuting offenders.
- Assisting in managing the school.

It will achieve this by:

- Providing evidential quality images of criminal incidents and suspects.
- Assisting the responsible authorities in the investigation of crime and disorder.

Data Protection

The system shall be used in accordance with all relevant laws and guidelines, including the Data Protection Law (Jersey) 2018.

Signage

Signs are displayed at entrance points and within the area covered by the system to inform staff, students and the public.

Management of the system

The overall management of the system is the responsibility of the Principal of the service, who has appointed the Business Manager for the function of Data Controllers.

Management and operation of control equipment

The system will be managed in accordance with all relevant legislation.

Access and security

The day-to-day management and security of the control equipment and data is the responsibility of the Business Manager who will follow the data protection guidelines with regards to access to the "Control Room" by visitors.

Incident reporting

A register of incidents and reviews shall be stored in the Business Manager's office and maintained by the Business Manager who will ensure that details of any incidents relating to the use of the system are logged.

Incident response

During monitoring, if criminal or suspicious activity of a serious nature is observed then the Service should immediately inform the Police. Once an incident is reported to the Police it will be dealt with in accordance with Police procedure. All other incidents will be logged and dealt with by the relevant authorities. Only the Business Manager, Admin staff or members of the SMT will have access to the system and downloaded images.

Storage of recorded images and their viewing

- The storage space shall be dust and moisture proof.
- Viewing or copying will be carried out only if it would assist the service in supporting procedures for which the Principal is responsible or to address one of the issues in the "purpose of CCTV".
- Recorded images are not to be taken away from the service premises under any circumstance.
- A record of viewing and copying must be noted in the register of incidents and reviews.

The register of incidents and reviews

The register will include the following:

- When searching or reviewing an incident the purpose of doing so should be recorded. Also note if the search was successful or not.
- Who carried out the search and/or copied the event.
- Persons present (particularly when reviewing).
- Date, start and end time of the incident.
- Details of the time of the review/copy.
- Details of the officer or authorised agent collecting the copied media and their contact details.

- Date of collection along with a signature and name in block capitals, including agency.
- On occasion where the request relates to an ongoing incident or investigation any appropriate reference numbers should be included.

Access to recorded information

The Data Projection Art provides Data Subjects (individuals to whom "personal data" relates) with a right to have access to CCTV images relating to them. People can make a request to review their footage by making a Subject Access Request in writing to the service. Where Subject Access Requests are made on behalf of a data subject, a written signed consent will be required from the subject before access to the footage is provided.

Applications received from outside bodies (e.g. solicitors or Courts) to view or release recorded data will be referred to the Principal. In these circumstances' recordings will only be released where satisfactory documentation is produced to support the request. Requests from Parents will only be granted where only their child is viewed and if CCTV footage has other children the request cannot be granted.

A fee will be charged for the provision of stored data, £10 for Subject Access Requests and a sum not exceeding the cost of materials in other cases.

Staff training

The Principal shall ensure that all appropriate staff are trained in the use of the equipment and are familiar with their data protection responsibilities as detailed in the ICO's CCTV Code of Practice 2008.

Complaints

- Any safeguarding concerns regarding the access and use of the service's CCTV system should be recorded and reported to the CPLO.
- Any complaints about the service's CCTV system should be addressed to the Principal.
- Complaints will be investigated in accordance with this policy.

Breaches of the policy

- Misuse of a recorded image or the system will be a disciplinary offence.
- Any breaches of the policy by service staff will be individually investigated by the Principal and appropriate disciplinary action taken.
- Disciplinary action can also include prosecution under the Data Protection Act and criminal proceedings.