SUPAJAM
GATEWAY TO MUSIC
MUSIC EDUCATION FOR 16 TO 25 YEAR OLDS

Ofsted
Good
Provider

CCTV Policy March 2022

Reviewed June 2022

(To be reviewed August 2022)

Policy statement
This policy seeks to ensure that the Close Circuit Television (CCTV) system used at SupaJam is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation 'GDPR" and the Data Protection Act 2018 "DPA 2018"), and includes the principles governing the processing of personal data as set out in Appendix 1.

It also seeks to ensure compliance with privacy law.

It takes into account best practice as set out in the codes of practices issued by the Information Commissioner Office (ICO) and by the Home Office.

SupaJam uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out below.

CCTV surveillance at the college is intended for the purposes of:

- promoting a safe SupaJam community and to monitor the safety and security of its premises
- protecting the college buildings and college assets, both during and after college hours
- promoting the health and safety of staff, students and visitors as well as monitoring student behaviour
- preventing bullying
- reducing the incidents of crime and anti-social behaviour (including theft and vandalism), supporting the Police in a bid to deter and detect crime

The system comprises of:

- 49 fixed cameras at the Swanley base
- 15 at Canterbury base
- Brighton base does not yet have any CCTV cameras

The CCTV system is owned and operated by the college and its deployment is determined by the college Senior Leadership Team (SLT). The college's CCTV Scheme is registered with the Information Commissioner (ICO) under the terms of the Data Protection Act.

The CCTV monitoring stations are situated in the reception room within the Swanley base, and the printing room within the Canterbury base. Access to CCTV is restricted and the process of requesting access is outlined below.

This policy assumes that:

- All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images.
- All operators are trained in their responsibilities of handling data accessed through the use of CCTV.
- All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited

by this policy e.g. CCTV will not be used for monitoring employee performance or to monitor normal teacher/student classroom activity.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the College, including Equality & Diversity Policy, codes of practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

Justification for use of CCTV:
The use of CCTV to control the perimeter of the college buildings for security purposes has been deemed to be justified by SLT. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation or of antisocial behaviour. SupaJam captures images which include a public footpath for the security, safety and reputation of the organisation.

In other areas of the college where CCTV has been installed, e.g. hallways and stairwells, the college has demonstrated via a DPIA that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that may have arisen prior to the installation of the system.

Data Protection Impact Assessments (DPIA)
Where new CCTV systems or cameras are to be installed, the college will carry out a full DPIA identifying risks related to the installation and ensuring full compliance with data protection legislation. This may involve the need for consultation with staff, parents and local residents.

Where existing CCTV systems are in operation as of 2018 (Swanley) and 2019 (Canterbury), the college will endeavour to carry out a full DPIA on any upgrade or replacement of the system or within a 3 year period from the date of the implementation of GDPR, whichever is sooner.

Location of cameras
Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.

The college will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act. The college will make every effort to position cameras so that their coverage is restricted to the college premises, which may include outdoor areas. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify, and therefore there are no cameras located in the bathrooms. SupaJam has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals.

Covert surveillance:

The college will not engage in covert surveillance.

Notification:
A copy of this CCTV Policy is available on the staff shared drive and will be provided on request to students, parents and visitors to the college and will be made available on the college website.

Adequate signage indicating the use of CCTV will also be prominently displayed at the entrance to the college property. Signage shall include the name and contact details of the data controller. Appropriate locations for signage will include:

- at entrances to premises i.e. external doors,
- reception area
- at or close to each internal camera

Storage, Retention and Access
The images captured by the CCTV system are automatically deleted after a period of no more than 30 days (but often sooner, as the system rewrites and may only store up to 14 days in periods of high activity). There will also be circumstances where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue. The images/recordings will be stored digitally on the Drive, with access only to those necessary for the purpose of retaining that data i.e. staff involved in using the footage as part of an investigation.
When storing CCTV, it will be placed directly in the 'Downloaded CCTV' folder on the drive, which can be accessed on request via the DPL. CCTV footage will be labelled with the date of the footage and any data subject initials that the footage is relevant to.

Access to all CCTV (including retained CCTV) will be restricted to authorised personnel, supervised by the Centre Managers and DPL (who may delegate this responsibility to the Deputy Centre Managers or another member of SLT).
Staff may request authorisation to view the CCTV by the following process:

- Email the Centre Manager or DPL the reason for your request. Does it meet one of the intended purposes for SupaJam's use of CCTV?
- The Centre Manager or DPL will log your request in the appropriate log book and respond to your email with whether or not they have decided to authorise it. If they do not feel the request is justified, they will deny it and give you a reason why. This is to protect the personal data stored within the system under the Data Protection policy.
- If your request is authorised, the Centre Manager or DPL will allocate a second member of staff to view the CCTV footage with you at an agreed time. You must not access CCTV footage for any reason other than outlined within your request.
- You must treat the information accessed as you would treat any other personal data.

The CCTV Access Request Log Book will record:

- The date of the access request
- The name of the member of staff requesting access
- If an external body (such as the police) the organisation that they represent
- The reason why the staff member is requesting access
- Whether the request is a SAR (Subject Access Request) and, if granted, how the data is going to be shared with the data subject
- Whether access has been granted

- If granted, the second member of staff who will support access
- The date and time at which the CCTV is accessed
- The signature of the Centre Manager or DPL overseeing the request
- Where the Centre Manager or DPL is the member of staff accessing the CCTV, they will be allowed to authorise their own access but will still require a second member of staff to accompany them.

In relevant circumstances, CCTV footage may be accessed:

- By the police where the college is required by law to make a report regarding the commission of a suspected crime
- Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the college property
- To the HSE and/or any other statutory body charged with child safeguarding
- To data subjects (or their legal representatives), pursuant to a Subject Access Request or individuals (or their legal representatives) subject to a court order
- To the school insurance company in order to pursue a claim for damage done to the insured property.
- By the CCTV installation company where repairs may need to be conducted or new cameras may need to be placed etc.

Subject Access Requests (SAR):
Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act. A record of the SAR request will be kept within the CCTV Access Request Log Book.

Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

The college will respond to requests within 30 calendar days of receiving the request in line with the Data Protection policy.

The college reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals, jeopardise an on-going investigation or where it includes the personal data of another individual.

In giving a person a copy of their data, the college will provide a series of still pictures or a video via a digital format.

Complaints
Complaints and enquiries about the operation of CCTV within the college should be directed to the Centre Manager/DPL in the first instance.

Staff training
The Centre Manager, Deputy Centre Manager, SLT and DPL will receive additional training to ensure they comply with this policy.
All staff will be trained in the appropriate handling of data via GDPR training to ensure they understand that all information relating to CCTV images must be handled securely.
If a member of staff misuses the surveillance system information, this will lead to an investigation and may lead to disciplinary proceedings.

Responsibilities:
The Centre Manager, DPL or appropriate delegates will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by the college
- Oversee and coordinate the use of CCTV monitoring for safety and security purposes within the college
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance alongside this policy
- Ensure that the CCTV monitoring at the college is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a CCTV Access Request Log Book
- Ensure that monitoring recorded tapes are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the college and be mindful that no such infringement is likely to take place
- Cooperate with the college DPL in reporting on the CCTV system in operation within the college
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”
- Ensure that monitoring footage are stored in a secure place with access by authorised personnel only
- Ensure that images recorded are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual’s reasonable expectations.

Should you have any questions or concerns regarding this policy or SupaJam’s use of CCTV, please contact the Data Protection Lead (Becca Walker):

becca.walker@supajam-education.org

Appendix 1

Principles relating to the processing of personal data under the Data Protection Act 2018 and General Data Protection Regulation (GDPR)

Personal data shall be:

- Processed lawful, fairly and in a transparent manner in reaction to the Data Subject
- Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.