SHREWSBURY COLLEGES GROUP

CCTV POLICY

Contents

SHREWSBURY COLLEGES GROUP

CCTV POLICY

1. INTRODUCTION

1.1. Shrewsbury Colleges Group (SCG) captures and records video images (CCTV) and uses Body Worn Video Camera devices (BWVC) to support a safe and secure environment for student, staff and visitors, and to protect college property, students, staff and visitors.

2. PURPOSE OF CCTV

2.1. SCG has installed CCTV systems to:

- Ensure staff and student safety and security.
- Assist in the deterrence, prevention, detection and prosecution of crime.
- Provide objective evidence which may be used, subject to application of the appropriate disciplinary procedure, as part of disciplinary proceedings involving staff or students to support or refute allegations of misbehaviour or misconduct.
- Monitor security of campus buildings and vehicle movement problems around the campuses.

Guidance

Before installing and using CCTV on SCG premises, the following steps should be taken:

(i). Assess and document the appropriateness of, and reasons for, using CCTV.

(ii). Establish and document the purpose of the proposed scheme.

(iii). Establish and document who is responsible for day-to-day compliance with this policy.

(iv). Because CCTV involves the processing of personal data, register the scheme with the data protection officer before using the system.

3. COVERT RECORDING

3.1. SCG may undertake covert recording where:

- There is reasonable cause to suspect that an illegal or unauthorized action(s) is/ are taking place or about to take place: And where;
- Informing the individual(s) concerned that the recording is taking place would seriously prejudice the reason for making the recording;
- Intentional Covert recording may only be undertaken with the written authorization of either the Principal, Executive Director of Finance, or Vice Principal Quality, Apprenticeships and Information.

Guidance

Any such monitoring will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring, and only for specific unauthorized activity.

All such occasions will be fully documented showing who made the decision to use covert monitoring and why.

4. CAMERAS AND BODY WORN VIDEO CAMERAS

SCG will make every reasonable effort to position cameras so that CCTV cameras do not cover areas outside SCG property in line with the purposes set out in 2.1 above. Cameras with pan and zoom functionality may be redirected if it is suspected that activities with a safeguarding, safety or security concern, or if illegal activity is suspected to be occurring.

SCG will clearly display signs so that staff, students and visitors are aware they are in an area covered by CCTV.

Where deemed necessary, the College will use portable devices and body worn video camera (BWVC) devices to support the purposes set out in section 2.1. Where portable or BWVC devices are intentionally deployed covertly this shall only be with the written approval of either the Principal, Executive Director of Finance, or Vice Principal Quality, Apprenticeships and Information. Use of BWVC devices will normally be restricted to individuals with a security aspect to their role.

Where body worn devices are used this will be done openly. Users must always ensure that BWVC is only used as an overt audio or overt visual recording mechanism and is not intentionally used covertly.

Use of BWVC

<u>Starting recording</u>

Staff should recognise when a situation is beginning to escalate and must consider starting to record as early as possible, which may act as a de-escalation tactic. Staff should make a verbal announcement that they have begun recording to ensure those captured by the camera lens/microphone are aware they are now being recorded.

BWVC does not replace the need for written statements. BWVC footage is to support and not replace written statements.

Users must record the justification for the use of the camera in a daily log and note use of BWVC in any written incident statements.

<u>During recording</u>

Upon activating their BWVC, users must make a clear verbal announcement to anyone in the vicinity that the recording of both audio and visual images is taking place. This must take place as soon as it is possible and safe to do so. If the BWVC is activated prior to arriving at the scene of an incident, then the announcement must be made to those at the scene once it is possible and safe to do so.

For example such an announcement might be: “everything you say and do is now being recorded for your safety and the safety of others”.

Recording must, where practicable, be restricted to those individuals and areas that are necessary to record to obtain material relevant to the incident or event. It is important that users minimise the risk of collateral intrusion on those not involved in the incident wherever possible. However, and importantly, this must not be at the expense of failing to obtain enough coverage of the incident/event or restricting the user’s movements and ability to manage the incident.

The use of BWVC in areas where there is a higher than usual expectation of privacy (such as toilets, showers, changing rooms, faith rooms and medical treatment rooms), will require compelling reasons for doing so, for example in response to an incident where the safety or security of others is at risk. Where footage is recorded in these areas’ consideration should be given to accelerated deletion of recordings not required as evidence for an investigation, or by placing restrictions on viewing the recording or pixilating/obscuring the recording at the earliest opportunity.

Any footage or recording should ideally be uninterrupted from the beginning of the incident until the end.

Where incidents or events are protracted and there are lengthy periods of inactivity or because of the need to isolate confidential details such as victim details or witness details from the footage, there may be cause to conduct selective filming. Users should be aware that this could lead to challenge and must ensure that explanation and justification is given for selective recording in the accompanying incident statements.

If using selective recording due to inactivity and where multiple BWVC are available users should consider having one camera continuing to record whilst others stop recording and explain their rationale for using selective recording on camera before switching any camera off.

Ceasing recording

In the same way that a user will record their decision to activate BWVC so too will the decision to cease recording be documented. In making this decision users must be satisfied that the risk of not capturing further helpful material is minimised. Under normal circumstances users must cease recording either when:

• The incident has concluded to a safe and secure position; or

• It is no longer justifiable, necessary, or proportionate to continue recording.

Any portable media containing images (e.g. SD cards) will be stored in a secure location accessible only to appropriate individuals.

Dealing with objections to being filmed

Any objection by a student(s), visitor(s) or other person to the use of BWVC to record, must be addressed by the BWVC user with a clear and concise explanation why recording is taking place.

The user must explain to the student(s)/visitor(s) the benefits of recording the encounter; which may include explaining that the recording is to safeguard all parties by ensuring an accurate reflection of any action or comments made by either party. Users may also direct visitors to the signage which explains that BWVC/CCTV is used in the establishment and in the case of a complaint to write to the Principal.

The user may also explain that non-evidential material is only retained for a maximum period of 30 days and that any access to the material is both limited and controlled;

BWVC material is restricted and may only be disclosed in line with section 6 below.

If the student or visitor continues to object, then the user must decide based on the circumstances of the incident or event. Stopping filming at the request of an individual would however be an exceptional occurrence and the normal policy would be to continue to film and to record the individual's objections on film and within any accompanying written document.

5. IMAGES

5.1. Quality

The quality of Images produced by the equipment will be reviewed on an ongoing basis and equipment replaced or upgraded so that images are effective for the purpose(s) for which they are intended.

5.2. Retention

For digital recording systems, CCTV images held on the hard drive of a PC or server will be overwritten on recycling basis once the drive is full, which is normally not more than 31 days.

Other Images stored on removable media such as CDs will be destroyed, or in the case of re-writeable storage media such as SD cards which is retained during an academic term will be erased during the following half-term unless the purpose of the recording remains relevant.

BWVC recordings will be overwritten on a recycling basis unless specifically stored in a designated secure area on the college network for the purposes of an investigation. BWVC recordings which are retained during an academic term will be erased during the following half-term unless the purpose of the recording remains relevant.

6. ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

6.1. Access to CCTV systems and stored BWVC recordings will be controlled by the Head of Technical Services. Disclosure of, images recorded on CCTV and BWVC recordings will be restricted and carefully controlled. This will ensure that the rights of individuals are retained, and also ensure that the images can be used as evidence if required. Images and recordings can only be disclosed in accordance with the purposes for which they were originally collected and in accordance with SCG's Notification to the Office of the Information Commissioner, or as otherwise required by law.

6.2. **Access to Images and BWVC recordings**

Access to recorded CCTV images and BWVC recordings will be restricted to those staff authorised to view them, and to other relevant staff when required, or as part of an investigation, in line with the purposes for which CCTV or BWVC is used (See section 2 above). Still images may be circulated by e-mail only to relevant staff as part of an investigation into an incident to assist with identification of individuals relevant to the investigation. Images shall not otherwise be made more widely available.

Monitors displaying images from areas in which individuals would have an expectancy of privacy should only be seen by staff authorised to use the equipment.

Viewing of recorded images will take place in places where appropriate confidentiality of images can be assured while viewing is occurring.

If media on which images are recorded are removed for viewing purposes, this will be documented.

Images retained for evidence will be securely stored.

Guidance

Document the following information should be when media is removed for viewing;

(i). Date and time the media is issued

(ii). The name of the person the media is issued to

(iii). The name(s) of the person(s) who are expected to be viewing the images contained on the media.

(iv). The name of SCG department to which the person viewing the images belongs, or the person's organization if they are from outside SCG.

(v). The reason for viewing the images

6.3. **Disclosure of images**

***The Principal, Executive Director of Finance or Vice Principal Quality, Apprenticeships & Information, or their designated agent, are the only people who can authorise disclosure of information to the police or other parties.**

Disclosure to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

- Police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/ or the prevention of terrorism and disorder*
- Prosecution agencies
- Relevant legal representatives
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
- In exceptional cases, to others to assist in identification of a victim, witness or perpetrator in relation to a criminal incident.
- Members of staff involved with college disciplinary processes.

Guidance

In addition to the information required in section 6.2 above, the following should be documented;

(i). If the images are being removed from the CCTV system for secure storage in another area, the location to which they are being transferred.

(ii). Any crime incident number, if applicable.

The signature (or electronic acknowledgement of receipt) of the person to whom the images have been transferred.

7. INDIVIDUALS' ACCESS RIGHTS

7.1. The Data Protection Act 1998 gives individuals the right to access personal information about themselves, including CCTV images.

All requests for access to images by individuals (when they are asking for access to images of themselves) should be made in writing to the SCG's data protection officer.

There will be an administration charge of **£10.00** for the provision of this information.

7.2. The manager responsible for the system will liaise with the data protection officer to determine whether disclosure of the images will reveal third-party information.

Under the Freedom of Information Act 2000, a copy of this policy will be provided to anyone making a written request for it.

Guidance

Requests for access to CCTV images must include:

(i). The date and time when the images were recorded

(ii). The location of the CCTV camera

(iii). Further information to identify the individual, if necessary

SCG will respond promptly and at the latest within regulatory time frames or within 30 days of receiving sufficient information to identify the images requested.

Staff responsible for CCTV systems will refer all such request to the Head of Technical Services. If SCG cannot comply with the request, the reasons must be documented. The requester will be advised of these in writing, where possible.

If there is any doubt about what information must be provided to enquirers, please contact the Head of Technical Services.

8. RESPONSIBILITY FOR CCTV and BWVC SYSTEMS

8.1. The overall responsibility for CCTV and use of BWVC lies with the Executive Director of Finance. Day to day responsibilities for CCTV lie with the Head of Technical Services. Day to day responsibilities for BWVC lie with the Commercial manager.

8.2. The users of the BWVC devices will have received basic instruction in the use of BWVC devices prior to any use. It is the responsibility of the BWVC user to ensure that:

- Equipment is checked prior to deployment to ensure it is working correctly.
- That the device batteries are charged prior to use and immediately recharged on return.
- That the time and date settings are accurate.
- That camera lenses are clean and the picture quality is suitable.
- The camera lens is aimed and focused appropriately to capture evidence.
- Compliance with legislation and guidance.
- View only footage they have a bona-fide reason for viewing.

8.3. The Commercial Manager shall be responsible for:

- The safe storage and issue of BWVC devices
- Ensuring that all documents associated with BWVC use, such as booking in/out, viewing of footage, deletion and recording logs conforms to this policy & procedure.
- Ensuring that viewing and retention of BWVC footage is appropriate and controlled in line with this policy and legislation.

8.4. Responsible for fault reporting and seeing that any faults with BWVC equipment are addressed at the earliest opportunity ensuring the BWVC equipment is available for use at all times.

9. STAFF TRAINING

9.1. The Head of Technical Services will ensure that staff handling CCTV images or recordings receive appropriate training on the operation and administration of the CCTV systems. In addition, they will liaise with the data protection officer to ensure training is provided on the implications of the Data Protection Act 1998 with regard to those systems.

9.2. The Commercial Manager will ensure that staff handling BWVC devices, images or recordings receive appropriate training on the operation and administration of the BWVC devices. In addition, they will liaise with the data protection officer to ensure training is provided on the implications of the Data Protection Act 1998 with regard to BWVC devices.

10. COMPLAINTS

10.1. Complaints and enquiries about the operation of the CCTV systems or BWVC devices should be addressed to those having day to day responsibility, as detailed in section 8 above.

Enquiries relating to the Data Protection Act should be addressed to the Data Protection Officer.

If a complainant or enquirer is not satisfied with the response received, they should write to the Data Protection Officer.

11. MONITORING AND COMPLIANCE

11.1. Annual reviews will be undertaken by the Head of Technical Services in respect of CCTV and by the Commercial Manager in respect of BWVC to ensure knowledge and compliance is kept up to date with current legislation.