| | |
|---|---|
| **Document No:** | **EC024** |
| **Issue No.** | **1** |
| **Issue Date:** | **2025-11-05** |
| **Renewal Date:** | **2028-11-05** |
| **Originator:** | **Director of Estates and Campus Services** |
| **Responsibility:** | **Deputy Principal Finance and Corporate Services** |

# SECURITY (BODY-WORN CAMERAS) POLICY

## 1. INTRODUCTION

1.1. Leicester College recognises the importance of providing a safe and secure environment for all staff, students and visitors to its sites. As part of the College's security strategy, a Body-Worn Camera (BWC) scheme has been introduced, and this Policy has been agreed to ensure that the scheme is operated:

1.2. fairly, lawfully and for the purposes authorised in accordance with the College's policy;

1.3. with due regard for the privacy of individuals who may be captured by BWCs; and

1.4. in accordance with the operational procedures designed to safeguard the integrity of the scheme.

1.5. The College will have due regard to the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, the Protection of Freedoms Act 2023, and the Human Rights Act 1998. Although not a relevant authority, the College will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012, and in particular the 12 guiding principles contained therein.

1.6. Leicester College respects and supports an individual's right to go about their lawful business, and this is a primary consideration when operating a BWC system. Although there may be some loss of privacy when a BWC is operational, this technology will not be used to monitor individuals during the ordinary course of their lawful business in the area under surveillance. Individuals will only be continuously monitored if there is a reasonable suspicion that a serious breach of College policy or an offence has occurred, may be occurring, or is likely to occur.

1.7. This policy should be read alongside the College's privacy notices, the Closed-Circuit Television Policy (EC004), the Data Protection Policy (GP002) and the Records Retention Policy (GP012).

## 2. DEFINITIONS

2.1. For the purposes of this policy, the following terms have the following meanings:

2.1.1. BWC: small, wearable cameras, typically worn on the chest of an individual and designed to capture audio enabled video footage of individuals and property.
2.1.2. BWC Data: information such as audio and video recordings.
2.1.3. Data Protection Officer: the person who advises the College on data protection compliance, monitors compliance with data protection laws.
2.1.4. Data subjects: all living individuals about whom we hold personal data as a result of the operation of the BWC system.
2.1.5. Personal data: data relating to an identified or identifiable living individual. In relation to the BWC system, this will include audio enable video images of identifiable individuals and static pictures.
2.1.6. Processors: means any organisations that process personal data on our behalf and in accordance with our instructions (for example, our service providers).
2.1.7. Processing: means 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.

## 3. POLICY STATEMENT

3.1. The purposes of the BWC scheme are to:

3.1.1. reduce the fear of crime or other unacceptable conduct and provide reassurance for all staff, students, and visitors to the College;
3.1.2. reduce antisocial behaviour;
3.1.3. assist in providing a safer environment for students, staff, and visitors to the College by reducing the threat to personal safety and property;
3.1.4. assist police in the detection, deterrence and prevention of crime and antisocial behaviour at the College by securing evidence to identify, apprehend and prosecute offenders;
3.1.5. provide evidence for internal disciplinary investigations and hearings;
3.1.6. reduce the potential for incidents to escalate;
3.1.7. assist in the investigation of allegations of inappropriate conduct by staff;
3.1.8. discourage aggressive and abusive behaviour.

3.2. BWCs will not be used for the ad-hoc monitoring of anyone.

3.3. To support the purposes of the scheme, BWC technology will be used by College staff for security purposes, when necessary.

## 4. MANAGEMENT AND ACCOUNTABILITY

4.1. Leicester College owns the BWC system and operates it at the Abbey Park Campus, Freemen's Park Campus, St. Margaret's Campus and outreach centres leased by the College.

4.2. All recorded material is owned by, and copyright of any material is vested in, the College.

4.3. The College's Estates and Campus Services Department, whose personnel are employed directly by the College, will operate this scheme.

4.4. The Deputy Principal Finance and Corporate Services is responsible for the overall management of the scheme and the requirements of the policy; the College Director of Estates and Campus Services will manage the scheme on a day-to-day basis.

4.5. The Estates and Facilities Manager or Facilities Co-ordinator shall be responsible for managing the scheme in terms of maintenance on a daily basis.

4.6. BWC Data may only be accessed by the following members of staff:

4.6.1. Campus Wardens;
4.6.2. Director of Estates and Campus Services, Estates and Facilities Manager or Facilities Co-ordinator; and
4.6.3. any other members staff who require access to BWC recordings as part of their role, and who are authorised by the Director of Governance and Policy (Data Protection Officer).

4.7. Access to or release of BWC Data will be strictly in accordance with the operating procedures approved by the Deputy Principal and should be authorised by the Deputy Principal Finance and Corporate Services or the Director of Governance and Policy (Data Protection Officer).

4.8. This policy is binding on all personnel (whether employees, volunteers, contractors or otherwise) and students of the College, all employees of contracted out services, and applies to all other persons who may, from time to time, and for whatever purpose, be present on the College's premises.

4.9. The College undertakes to comply with a requirement for accountability as set out in this policy and to consult with, and provide information to, interested parties regarding the operation of the scheme and any proposed changes to the scheme or policy.

4.10. The College will:

4.10.1. Approve and ensure compliance with, this policy and the operating procedure for the scheme (including the provision of copies of this policy when requested to do so by any person having legitimate grounds for so requiring them).

4.10.2. Provide adequate signage to notify persons entering areas monitored by the scheme that a BWC system is in operation.

4.11. The use of BWCs will be regularly evaluated to determine whether it is necessary and proportionate to continue its use.

## 5. USE OF PERSONAL DATA CAPTURED BY BWC

5.1. The College processes BWC Data lawfully, fairly and transparently, in compliance with data protection laws, including the processing principles set out in the Data Protection Policy and best practice recommended by the ICO.

5.2. All employees with access to personal data are adequately trained and aware of their responsibilities in relation to the use of personal data, including the procedures set out in this policy and in the Data Protection Policy.

5.3. BWC Data may be processed only for the purposes set out in paragraph 2.1 above, or for purposes which are compatible with those purposes. It will not be used for automated facial recognition.

5.4. To ensure security of BWC Data, the recordings are stored in a way that maintains integrity and confidentiality of BWC Data. This should include password protection and encryption.

5.5. We have procedures in place to facilitate the exercise of data subject rights (see paragraph 8 below).

5.6. We may engage processors to process personal data on our behalf. Where we do so, we will ensure that appropriate contractual safeguards are in place to protect the security and integrity of BWC Data.

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

5.8. Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording, it will only relate to the specific suspected illegal or unauthorised activity and will not continue after the investigation is completed.

## 6. RETENTION AND ERASURE OF BWC FOOTAGE

6.1. BWC Data will be uploaded and stored on the College's IT systems and will not be kept for longer than six weeks, except if the College has a specific lawful purpose for retaining it. For example, in instances where footage is being used for crime prevention purposes, or for use in disciplinary, insurance and/or legal proceedings, the data will be kept long enough for incidents to come to light and to fulfil the intended purpose.

6.2. At the end of their useful life, all BWC Data stored in whatever format will be erased permanently and securely. Any physical storage such as hard drives will be disposed of as confidential waste. Any still photographs and hard copy prints

will be disposed of as confidential waste.

## 7. THIRD PARTY ACCESS

7.1. Third party requests for access will be considered in line with the UK GDPR and the DPA 2018 in the following categories:

7.1.1. law enforcement agencies including the Police;
7.1.2. disclosures to public authorities in order to support their investigations;
7.1.3. disclosure required by law or made in connection with legal proceedings or, where appropriate, insurance claims;
7.1.4. disclosures in response to a subject access request.

7.2. All third party requests to access or view BWC Data will be considered on a case by case basis and strictly in line with UK data protection law.

7.3. In certain circumstances, we may allow law enforcement agencies, public authorities or other organisations with a statutory right to obtain information, to access BWC Data. In such cases, BWC Data will be disclosed only where there is satisfactory evidence that it is required for law enforcement proceedings or under a court order. Such evidence may include a form certifying that the images are required for an investigation, the prevention or detection of crime or the apprehension or prosecution of offenders, and that the investigation is likely to be prejudiced by failure to disclose the information. Where images are sought by other organisations with a statutory right to obtain or request information, evidence of that statutory right needs to be obtained before BWC Data may be disclosed.

7.4. The Data Protection Officer is responsible for ensuring that we maintain a record of all disclosures of BWC Data. Every disclosure of BWC Data must be recorded in the BWC logging file and the relevant details must include:

7.4.1. the name of the police officer or other relevant person in the case of other organisations accessing or receiving the copy of the recording;
7.4.2. brief details of the images captured by the BWC to be used in evidence or for other purposes permitted by this policy;
7.4.3. the crime reference number where relevant; and
7.4.4. date and time the BWC Data was made available to the police or other organisation.

7.5. No images from BWC cameras may be posted online or disclosed to the media.

## 8. DATA SUBJECT RIGHTS

### Right of Access

8.1. Data subjects have the right to request confirmation of whether we process their personal data and ask us to provide a copy of their personal data (known as making a ‘data subject access request’ or ‘DSAR’) - this may include their

personal data captured by the BWC system.

8.2. Data subject access request can be submitted in any form (including verbally) but to enable us to deal with such requests efficiently, all verbal requests should be documented and, if possible, the requestor should be asked to confirm their request in writing. To help us locate the relevant footage, we should encourage data subjects to indicate the date(s) and time(s) of the recording, the location where the footage was captured and, if necessary, information identifying the individual. We will need to respond to the request even if the requestor refuses to provide such details.

8.3. Before providing any personal data, we may to confirm the requestor's identity (for example, where the requestor is unknown to us). Additionally, where a request is submitted by a legal representative of the requestor, we will need to confirm that person's authority to act.

8.4. Any requests for access to BWC Data should be forwarded to the Data Protection Officer without any delay, and in any case within two working days. The Data Protection Officer will be responsible for responding to data subjects in accordance with the procedure relating to data subjects' requests, set out in our Data Protection Policy.

8.5. When deciding what personal data captured in BWC recordings should be disclosed, the Data Protection Officer should consider (seeking legal advice where appropriate), whether any potential exemption under the UK GDPR or the DPA 2018 applies. Care must be taken not to disclose third parties' personal data where consent has not been given and where it would not be reasonable to disclose third party's personal data without consent. In such cases, it may be necessary to apply redactions or withhold BWC Data entirely.

8.6. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the information about their rights to complain to the ICO and to bring a civil claim and all additional information required under the UK GDPR. It must be sent within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR by up to two months).

**Other rights**

8.7. In certain circumstances, personal data captured by the BWC system, may be within the scope of other requests from data subjects, such as requests to have their personal data erased, to restrict the processing of their personal data or the objection to the processing.

8.8. Any requests or objections should be forwarded to the Data Protection Officer without any delay, and in any case within two working days. The Data Protection Officer will be responsible for responding to the data subject within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR for up to two months) in accordance with the relevant procedure set out in our Data Protection Policy.

8.9. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the information about the rights to complain to the ICO and to bring a civil claim and all additional information required under the UK GDPR.

## 9. OPERATING PROCEDURE

9.1. All operators will receive training in the use of BWC technology, including:

9.1.1. the practical use of equipment;
9.1.2. operational guidance (e.g. when to commence and cease recording); and
9.1.3. the potential legal implications of using the equipment.

9.2. BWCs will be activated for recording when the operator:

9.2.1. has an engagement with student(s), staff, or members of the public which, in the opinion of the operator, is confrontational and where they believe they may be subjected to physical or verbal abuse; and
9.2.2. encounter a situation in which they are approached by students, staff, or members of the public in a manner perceived to be aggressive or threatening.

9.3. BWCs will be used in an overt manner and will be clearly identified to indicate that it is a device capable of recording visual and audio footage. BWCs will not be used in a hidden or covert manner otherwise than in compliance with this policy.

9.4. BWCs will only be worn by staff wearing College uniforms or clearly displaying College identification.

9.5. If questioned, the operator must confirm whether they are recording and be prepared to answer further questions about the processing of the data.

9.6. A verbal warning should normally be given when recording commences. This will ensure that both the maximum deterrent value is achieved, and that those being recorded are fully aware. There may be instances when issuing a verbal warning may escalate the incident, or put the operator in danger, in which case the operator may be expected to justify why a verbal warning was not given.

9.7. Other means of alerting individuals to the fact that a recording is being made may be used, such as visible signage on the premises or a warning light on the device or uniform.

## 10. COMPLAINTS AND BREACHES OF THE POLICY

10.1. The College may take disciplinary action against any employee or student who breaches this policy.

10.2. Any intentional or reckless interference with any part of the scheme (including cameras) may constitute a criminal offence and will be regarded as a breach of discipline.

10.3. Grievances and complaints concerning the operation of the scheme may be progressed through the College's complaints or grievance procedures or those contained within the general regulations and procedures affecting students.

## 11. GENERAL ENQUIRIES

11.1. Enquiries concerning this policy and/or the Body Worn Camera scheme should be directed to the Deputy Principal Finance and Corporate Services, Leicester College, Freemen's Park Campus, 145 Welford Road, Leicester, LE2 7LW.

## 12. COMMUNICATION AND REVIEW

12.1. This policy will be published on the staff intranet and will be available on request to other parties. It will be reviewed at least every three years.