ASKHAM BRYAN COLLEGE

CCTV Policy 2025 - 2027

Equality Impact Assessment: Askham Bryan College recognises the importance of the Equality Act 2010 and its duties under the Act. This document has been assessed to ensure that it does not adversely affect staff, students or stakeholders on the grounds of any protected characteristics.

1. DOCUMENT HISTORY

Date of Issue: 21st July 2025
Approved on: 24th June 2025
Next review: November 2027
Owner: Director of Estates and Facilities
Author: Legal and Compliance Adviser
Publication requirements: PUBLIC

2. INTRODUCTION

2.1 Askham Bryan College recognises that the use of CCTV, including Automatic Number Plate Recognition (or "ANPR") at York, can be an important tool that can be used to ensure the safety of its staff and students and also visitors to College premises. The use of CCTV and ANPR can also assist in both crime prevention and crime detection. At the same time, the College recognises that the use of CCTV, including ANPR, should be properly controlled to avoid the potential of misuse.

2.2 The Surveillance Camera Code of Practice (SCCoP), available from https://www.gov.uk/government/publications/update-to-surveillance-camera-code, provides a framework for the use of surveillance camera systems which includes (a) closed circuit television ("CCTV") or automatic number plate recognition ("ANPR") systems; (b) any other systems for recording or viewing visual images for surveillance purposes such as Body Worn Video ("BWV"); (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b). The SCCoP sets out 12 guiding principles, which operators of surveillance systems are expected to follow. The 12 Principles of the SCCoP are reproduced at Appendix C.

2.3 At all times, the College will ensure compliance with the SCCoP and its 12 Principles.

2.4 No cameras, including webcams and Ring Doorbells, may be installed or operated on College premises by College students, employees or agents for the purposes of security or safety other than cameras linked to the College CCTV and ANPR systems, and cameras situated in the Wildlife Park, used for live streaming. Personal mobile phones and other personal devices such as spy cams should not be used for surveillance activity.

3. SCOPE

3.1 This policy applies across all sites where CCTV and ANPR systems are in operation, with the exception of Saltaire, whose systems are managed by Shipley College, and to all staff, students, contractors, agents, visitors and any other persons who may be present on College premises. For details of how Shipley College uses cctv footage and images, please see its Data Protection Policy which is available at https://www.shipley.ac.uk/media/e4dmrscc/data-protection-policy-23-25-1.pdf

4. PURPOSE

4.1 The use of CCTV, including ANPR, is primarily for the purposes of; but not limited to:

4.1.1 ensuring a safe environment for staff and students and visitors to the College and to assist the College in meeting its obligations under safeguarding legislation;

4.1.2 assisting in detecting and deterring crime, and in appropriate circumstances, to provide evidential material for court proceedings and assist with the prosecution of offenders;

4.1.3 assisting with Health and Safety investigations in the event of an accident;

4.1.4 assisting with the overall management of College buildings and land within the College boundaries, across all its sites, and to ensure they are kept free from vandalism, intrusion, damage and disruption;

4.1.5 assisting the police, Fire, Ambulance and Civil Emergency Services with the efficient deployment of their resources in the event of an emergency; and

4.1.6 where necessary, investigating disciplinary matters involving staff and or students.

5. CCTV SYSTEM

5.1 The CCTV system comprises a number of fixed and fully functional cameras located in buildings and externally around the main campus at York and at other sites.

5.2 Cameras, however, will not focus on private homes, gardens, and other areas of private property.

5.3 The system for cameras at York is managed by the Senior Estates and Facilities Manager, with support from an external supplier and is in operation 24 hours a day, 365 days of the year. The Senior Estates and Facilities Manager maintains a list of users and can allocate cameras to particular users. What users are able to see will depend on their area/function within the College. For instance, Student Services has access to all cameras for safeguarding purposes, as does the Estates team; but individual departments, such as Equine, will only have access to cameras relevant to their area of responsibility. All users have “live” reviewing rights; but only of their allocated area unless otherwise required. Wildlife Park cameras are managed by the

Digital Teaching, Learning and Innovation Lead. The systems at Gateshead and Stewart Park are managed by the Estates Project Manager who is responsible for allocating access to cctv to users at these sites.

5.4 Warning signs, as required by the Information Commissioner's Office CCTV Code of Practice, have been placed at strategic points, such as entrances and exits to various buildings, and main thoroughfares, where they are covered by the College CCTV system, and will inform staff, students and visitors that CCTV is in operation, why it is in operation and provide the contact details for the College's Data Protection Officer, in the event they have any complaints or queries.

5.5 The CCTV system is designed to ensure maximum effectiveness and efficiency; but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

5.6 Materials or knowledge secured as a result of the use of the CCTV system will not be used for any commercial purposes. Images may be released to the police, on request, for the use of investigation of a specific crime. Images will not be released to the media, including social media, for the purposes of entertainment, or otherwise.

6. ANPR

6.1 ANPR automatically reads vehicle number plates or vehicle registration marks (VRMs) at the time of access and egress to the College premises for comparison against database records. The police and government agencies use ANPR as a tactical option to disrupt, prevent and detect criminal activity. ANPR is also used by commercial companies, for example, garages, shopping centres and car parks. ANPR cameras at York are located at the Entrance of the Main Drive, The Farm Road & Horticulture Entrance.

6.2 The ANPR system will only be used to identify vehicle number plates and time of access and egress.

7. STORAGE OF IMAGES AND RETENTION

7.1 All images recorded on the College's CCTV cameras are digitally stored on College servers managed by the Senior Estates and Facilities Manager. Although the images can be searched, it is not possible to tamper or alter them. The ANPR images are also stored on the system and can be searched but not altered.

7.2 In the event of the police requiring CCTV images or ANPR footage, they can be provided, on receipt of the appropriate Data Protection form. Members of the public will need to make a Subject Access Request, ideally using the form at Appendix A.

7.3 The CCTV images over record after 30 days[1], however any relevant images can be locked on the hard drive for future reference, provided the College is aware that this

[1] unless the server is full, then that data could be overwritten, unless otherwise required for disciplinary, insurance or legal purposes, or there is some other valid justification for retaining the images/ footage for longer, and depending on when that request to save the footage is received

needs saving. ANPR images are kept for up to 30 days[2] and then purged from the system unless required for operational needs.

7.4 Viewing of live images on monitors is restricted to Estates and Facilities team, the IT team and other authorised personnel.

7.5 Images are viewed in confidence in secure private offices.

7.6 Requests to view images or image disclosure of third parties should be made in writing to the Legal and Compliance Adviser.

Reviewing footage

7.7 Any requests to review footage need to be reasonable. The College cannot be expected to review days or weeks' worth of footage.

8. USE OF BODY WORN VIDEO, PERSONAL MOBILE PHONES AND OTHER PERSONAL DEVICES SUCH AS SPY CAMS FOR SURVEILLANCE ACTIVITY

8.1 Body Worn Video ("BWV") cameras are small devices, usually worn on the chest, but sometimes concealed, that have the ability to capture both video and audio.

8.2 College policy is that BWV should not be worn by either staff, students or visitors to the College, which includes members of the public. This applies across all sites and centres.

8.3 Use of BWV in contravention of this policy raises a number of concerns, not least from a Safeguarding perspective; but also around data privacy.

8.4 Staff found to be using BWV in breach of this policy will be subject to disciplinary action under the Staff Disciplinary Policy. Students found to be using BWV in breach of this policy will be subject to the College's Support for Continuing Studies Policy and Procedures. Visitors/members of the public found to be using BWV in breach of this policy will be asked to leave site and must provide any footage to the College's Data Protection Officer. If necessary, the police will be involved.

8.5 Personal mobile phones and other personal devices such as spy cams should not be used for surveillance activity.

8.6 Staff found to be using personal mobile phones and other personal devices such as spy cams for surveillance activity will be subject to disciplinary action under the Staff Disciplinary Policy.

8.7 Students found to be using personal mobile phones and other personal devices such as spy cams for surveillance activity will be subject to the College's Support for Continuing Studies Policy and Procedures.

[2] unless otherwise required for disciplinary, insurance or legal purposes, or there is some other valid justification for retaining the images/ footage for longer, and depending on when that request to save the images is received

8.8 Visitors/members of the public found to be using personal mobile phones and other personal devices such as spy cams for surveillance activity will be asked to leave site and must provide any footage to the College's Data Protection Officer. If necessary, the police will be involved.

9. COVERT MONITORING

9.1 Covert monitoring is where the individual is not aware the monitoring is taking place and will only be justifiable in exceptional circumstances where there are grounds to suspect criminal activity or extremely serious malpractice.

9.2 Covert monitoring will only be permitted:

(a) with the prior approval of either the Principal and Chief Executive, Chief Finance Officer, Director of Governance or Executive Director of People and Organisational Development and

(b) where a lawful basis for the covert monitoring has been identified.

9.3 The decision to undertake covert monitoring must be fully documented and will set out how the decision to use covert recording was reached and by whom.

9.4 Covert monitoring will only be carried out for a limited period of time only and must be consistent with the objectives of undertaking the covert monitoring, i.e. it is necessary and proportionate means to investigate the suspected illegal or unauthorised activity.

9.5 Areas where a high level of privacy is expected will remain private and only limited numbers of people will be involved in the monitoring.

10. RESPONSIBILITIES

10.1 Maintenance of the physical CCTV system (cameras and equipment) and sites where the cameras are situated are the responsibility of the Estates and Facilities department. Cameras are checked regularly to ensure that they are functioning.

10.2 In terms of monitoring, only staff that have been set up as a user by the Senior Estates and Facilities Manager will be permitted to view or review any CCTV and ANPR. Typically, this will be:

At **York**:

- the Vice Principal (Students), Student Services Manager, senior members of the Student Services team, the Safeguarding Officer and designated safeguarding officers, in relation to any incidents involving students/any safeguarding incidents;

- the Executive Director of People Services and Organisational Development, the Head of People Operations and People Business Partners in relation to incidents involving staff, relating to staff disciplinaries, enforcement of People Services policies and procedures, etc;

- the Director of Estates and Facilities, Senior Estates and Facilities Manager, and members of the Estates team, in relation to incidents on College premises/affecting the College estate, and ANPR at York;

- the Residential Services Manager and deputies, Vice Principal (Students), Student Services Manager and the Senior Estates and Facilities Manager, in relation to any safeguarding incidents in relation to students in residential accommodation[3];

- College Security (all cameras – live images only);

- the IT team;

- the Health and Safety Manager in relation to any accidents that may occur on College premises, including at other sites where there is CCTV;

- Reception staff and LRC staff;

- Equine staff for safeguarding purposes and to ensure the health, safety and wellbeing of staff and students in that part of the campus;

- the Farm Manager (live footage of areas associated with Westfield Farm);

- and the Legal and Compliance Adviser in relation to any incidents that may need to be reported to the College's insurers and in response to any requests for CCTV footage to be disclosed in the event of a Subject Access Request (see section 11);

- but may also be any member of staff who may, from time to time, be authorised by the Vice Principal (Students), Executive Director of People Services and Organisational Development, the Principal and Chief Executive and Director of Governance, to review any footage, depending on the circumstances in which they are asked to do so *provided* there is a lawful basis for that individual to be authorised to view or review the CCTV (or ANPR footage) and the College can justify that decision.

At **Stewart Park**:

- the Head of Middlesbrough Campus and the Campus Operations Manager or any member of staff authorised by them. In the absence of the Campus Operations Manager, the Campus Administration Officer will have access;
- the LRC staff have access to live footage of the library; but there is no playback facility.
- the Estates Project Manager also has access to CCTV footage at Stewart Park.

[3] The College will ensure that any use of surveillance equipment (e.g. CCTV cameras) or patrolling of buildings or grounds for security purposes does not intrude unreasonably on residents' privacy, is known to students and their parents and is compliant with legislative requirements/restrictions (para 5.8 Further education residential accommodation: national minimum standards)

At **Saltaire**:

- the Head of Animal Management or any member of staff authorised by them.

At **Gateshead**:

- Head of Vet Nursing or any member of staff authorised by them. Also the Estates Project Manager.

Please note: with the exception of the Principal and Chief Executive, Vice Principal (Students), the Executive Director of People Services and Organisational Development and People Services team, the Director of Estates and Facilities, the Senior Estates & Facilities Manager and the Health and Safety Manager, the staff referred to above will only have access to their responsible areas. They will not otherwise be able to access/view footage from other areas/sites/departments.

10.3 Staff with the responsibility of reviewing any CCTV footage or ANPR are required to undertake their responsibilities strictly in accordance with this Policy, and the associated Procedures.

10.4 Breach of this Policy and the associated Procedures by any member of staff may result in disciplinary action.

11. SUBJECT ACCESS REQUESTS

11.1 Images caught on CCTV capture information about individuals and how they behave and can in some circumstances amount to Personal Data where it is possible to identify an individual(s) from that footage. As such, those images/that footage can fall to be disclosed in response to a Subject Access Request.

11.2 A valid Subject Access Request can be made verbally or in writing, and to any member of staff. However, to ensure that any Subject Access Requests for recorded material are properly responded to within the statutory time limit of one month, they should be forwarded immediately upon receipt to the College's Data Protection Officer (judith.clapham@askham-bryan.ac.uk) and to the College's Legal and Compliance Adviser (jethro.powell@askham-bryan.ac.uk).

11.3 Where possible, the person making the request ("the Requester") should be encouraged to make use of the form at Appendix A, as this will help to confirm contact details and specifics as to the material being sought such as date, time and location of camera(s), etc. However, there is no obligation on the Requester to use this form. The police will need to use the form at Appendix B.

11.4 As per the College's policy and procedure on Subject Access Requests, the Legal and Compliance Adviser and Director of Governance will have overall responsibility for responding to any Subject Access Requests.

11.5 Any footage that is ultimately located will then be saved to a USB memory stick which must then be password protected before it is sent to the Requester via registered post unless the Requester has asked for the footage to be sent by email, and it is possible to do so.

11.6 The password for the USB will be sent by separate medium, e.g. email or text/via phone call, or by letter, and will only be provided once the Requester confirms safe receipt of the USB.

11.7 **There will be no obligation to respond to the request for copy CCTV footage until such time as the Requester confirms their name and address.**

Saltaire

11.8 For requests for cctv footage at Saltaire, requests must be made to Shipley College. Please see Shipley College's Data Protection Policy for further details, which is available at https://www.shipley.ac.uk/media/e4dmrscc/data-protection-policy-23-25-1.pdf

12. FREEDOM OF INFORMATION ACT REQUESTS

12.1 As a public authority within the definition of paragraph 53(1) of Schedule 1 of the Freedom of Information Act 2000 (FOIA 2000), the College may also receive requests for information under the FOIA 2000 that may ask for recorded material to be disclosed. All such requests should be forwarded to the College's Legal and Compliance Adviser (jethro.powell@askham-bryan.ac.uk), copying in the Data Protection Officer (judith.clapham@askham-bryan.ac.uk), so that that request can be responded to within the statutory time limit of 20 working days.

12.2 Section 40 of FOIA 2000 contains a two-part exemption, however, relating to information about individuals.

12.3 If the College receives a FOIA request for surveillance system information, it will consider the following questions:

- **Is the information Personal Data of the person making the request?**

  If so, then that information is exempt from the FOIA 2000. Instead, the College will treat this request as a Subject Access Request instead.

- **Is the information Personal Data of other people?**

  If it is, then this material can only be disclosed if:

  - disclosure does not contravene one of the data protection principles;
  - disclosure does not contravene an objection to processing;
  - the information is not exempt from the right of access.

12.4 In practical terms, if individuals are capable of being identified from the relevant surveillance footage, then it is Personal Data about those individuals and the recorded material will not ordinarily be disclosed, unless those individuals consent to its disclosure, or there is some other lawful reason why the material might still be disclosed to the Requester.

12.5 Where the information includes Personal Data of third parties, the College will consider whether it is possible to apply redaction techniques to obscure images, before any

images or recorded material are disclosed. It may be appropriate to do this rather than exempting the information.

12.6 Information about what *surveillance systems* the College operates is, however, a request for information under the FOIA 2000 and will be responded to within the statutory time limit of 20 working days, unless one or more exemptions apply.

13. DATA PROTECTION

13.1 The operation of the system has been registered with the Information Commissioner's Office in accordance with current data protection legislation.

13.2 Images caught by College surveillance systems, where they show an identifiable individual, are "Personal Data" as defined by the Data Protection Act 2018 and the UK GDPR (see Article 4(1) UK GDPR). This policy must therefore be read in conjunction with the College's Data Protection Policy, and, where relevant, any associated policies and procedures.

13.3 All Personal Data will be processed in accordance with the data protection principles as set out in the UK GDPR and Data Protection Act 2018:

a) all Personal Data will be processed fairly and lawfully and in a transparent manner;

b) Personal Data will only be processed for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;

c) Personal Data will be adequate, relevant and limited to what is necessary for the purposes for which it is processed (data minimisation);

d) Personal Data will be accurate and where necessary kept up to date;

e) Personal Data will be kept in a format that permits identification of Data Subjects for no longer than necessary for the purposes for which the Personal Data is processed;

f) procedures will be implemented to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.

13.4 In addition, individuals will be allowed access to information held about them and, where appropriate, will be permitted to correct or erase it.

13.5 The lawful bases for any processing of Personal Data by College surveillance systems are (a) that it is in the College's legitimate interests to operate surveillance systems (for the purposes of prevention and detection of crime, and the safety and security of staff, students and visitors to College premises, and (b) to ensure that the College is meeting its statutory obligations under Health and Safety and Safeguarding legislation.

13.6 For the purposes of the Data Protection Act 2018, Askham Bryan College is the Data Controller.

14. HUMAN RIGHTS

14.1 The College recognises that operation of the College surveillance systems may be considered an infringement on privacy and acknowledges its obligations under the Human Rights Act 1998.

14.2 The College, however, also recognises its obligation to provide a safe environment for staff, students and visitors, and regards the use of surveillance systems within the College as a necessary, proportionate and suitable tool to meet its obligations to staff, students and visitors to College premises, for the reasons set out at 13.5 above.

14.3 College surveillance systems will only be used as a proportional response to identified problems and may only be used insofar as is necessary, and where appropriate, in the interests of national security, public safety, the prevention and detection of crime or disorder, the protection of health, the protection of the rights and freedoms of others, the management of buildings and land, and assistance in the resolution of a factual disagreement which emerges during investigation of a grievance, complaint or disciplinary allegation.

14.4 College surveillance systems shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

15. COPYRIGHT

15.1 The College retains ownership of copyright and of all material recorded by the system.

16. COMPLAINTS

16.1 Complaints should be made in accordance with the College's Complaints Policy available at https://www.askham-bryan.ac.uk/the-college/complaints. A physical copy of the College's Complaints Policy is available on request.

17. REVIEW

17.1 This Policy and the arrangements that underpin it will be reviewed every 2 years by Director of Governance and the Legal and Compliance Adviser.

18. SUPPORTING/RELATED DOCUMENTS

Further education residential accommodation: national minimum standards: National minimum standards for the accommodation by further education colleges and 16-19 academies of students aged under 18 (in force from 1st September 2018)

19. RELEVANT LEGISLATION

- Data Protection Act 2018
- UK General Data Protection Regulation ("UK GDPR")
- Health and Safety at Work etc. Act 1974
- Equalities Act 2010
- Police and Criminal Evidence Act 1984
- Criminal Justice and Public Order Act 1994
- Criminal Procedure and Investigations Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Regulation of Investigatory Powers Act (RIPA) 2000
- Freedom of Information Act 2000
- Sexual Offences Act 2003
- Protection of Freedoms Act 2012
- Home Office CCTV Operational Requirements Manual 2009
- Surveillance Camera Code of Practice (SCCoP) (2021)
- Information Commissioners Office (ICO) In the picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information 2017

20. RELATED POLICIES AND PROCEDURES

- Data Protection Policy
- Subject Access Request Policy
- Subject Access Request Procedure
- Data Retention Policy
- CCTV Procedures
- Safeguarding Policy
- Safeguarding Procedures
- Support for Continuing Studies Policy
- Support for Continuing Studies Procedure
- Student Recording of Lectures Policy
- Staff Disciplinary Procedure
- Complaints Policy
- Compalints Procedure
- HE Student Complaints Policy
- Health and Safety Policy and associated procedures

APPENDIX A

Subject Access Request Form (CCTV)

The Data Protection Act 2018 gives individuals a right of access to their Personal Data which is held by the College. In order for us to process such a request, please complete and return this form to the address below. If you have any queries, please contact the College's Legal and Compliance Adviser by phone on 01904 772238 or by email jethro.powell@askham.bryan.ac.uk .

1. Details of the Data Subject *(i.e. the person who is the subject of the Personal Data)*

Full name: _____

Address: _____

_____

Telephone number: _____

Email address: _____

Relationship to the College (eg "current student" or "job applicant"): _____

Student number or staff payroll number (if applicable): _____

If you are a member of staff, do you mind being contacted by internal email/phone about this request? ❑ Yes ❑ No

2. Are you the Data Subject? ❑ Yes ❑ No

YES: If you are the Data Subject please supply evidence of your identity, e.g. a photocopy of your student card, staff card or driving licence.

NO: Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed. We reserve the right to verify this directly with the Data Subject. If you do not have the Data Subject's written authority, what other legal justification have you for seeking access to this data?

Please note that the College may request additional information to confirm the identity of the data subject and/or requester as necessary.

3. Details of the person making the request (if different from question 1)

Full name:

Address: _____

_____

_____

Telephone number: _____

Email address: _____

4. Please describe the information that you are seeking, together with any other relevant information which will help us to identify the information you require. You should provide as much detail as possible. Attach an additional sheet if necessary.

5. Declaration. To be completed by all applicants.

I confirm that the information given on this form is accurate and complete. I understand that it is necessary for the College to be satisfied as to the identity of the Data Subject and/or the person making the request, and it may be necessary to obtain more detailed information in order to locate the correct Personal Data.

Signature: _____

Date: _____

Please return the completed form to the address on the previous page. You must enclose:

- evidence of your identity
- evidence of the Data Subject's identity (if different)
- authorisation from the Data Subject to act on their behalf (if applicable)

APPENDIX B

Request by Police for Disclosure of Personal Data to the Police

Under Schedule 2 Part 1 Paragraph 2 Data Protection Act 2018 and GDPR Article 6(1)(d)

SECTION A - TO BE COMPLETED IN FULL BY THE POLICE

Police reference: ……..

From:

Rank/Number/Name: ……

Station:

……

……...

Date/Time: Click here to enter a date.

Phone (including extension): ……

Email: ……

Name of the Student and nature of the Personal Data requested. Please also specify (brief details) nature of the offence you are investigating

I can confirm that the Personal Data requested is required by me (tick as required):

- for the prevention or detection of crime [ ]
- for the prosecution of offenders [ ]
- protecting the vital interests of a person [ ]
- other; please specify (such as application for renewal of gun licence, etc):

……
……
……

I can confirm that the Personal Data requested above is needed for the purposes indicated above and failure to provide that information will be likely to prejudice those matters. [ ]

I can confirm that the individual(s) whose Personal Data is sought should not be informed of this request as to do so would be likely to prejudice the matters described above. [ ]

Signature: ……

Counter signature (Supervisor/Line Manager):

……

Rank/Number/Name: ……

For completion by Askham Bryan College staff:

I can confirm I have seen identification that reflects this request to be authentic. Yes / No* (*delete as necessary)

Please specify: ……

Signed: …….. Date: ……

Please print your name here: ……..

SECTION B - TO BE COMPLETED IN FULL BY ASKHAM BRYAN COLLEGE REPRESENTATIVE

Only to be completed on receipt of a formal request from the Police; all requests must be approved by the Director of Governance, Legal and Compliance Adviser and or a senior manager prior to the release of the data.

Personal Data Release Summary

Askham Bryan Manager recommending the release of the Personal Data:

Name (please print): ……

Signature: ……

Date: ……..

Description of Personal Data including Special Category (or "sensitive") Data provided to the Police
State source of original data in College record system, e.g. whether ProMonitor or other system, records, etc
Please confirm how Personal Data was sent (e.g. Signed For, encrypted email, etc) and date sent

COMPLETED FORM TO BE RETURNED TO LEGAL AND COMPLIANCE ADVISER (HARD COPY/SCANNED COPY)

APPENDIX C

Surveillance Camera Code of Practice (SCCoP)

12 guiding principles of the Code:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be 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.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then 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.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date."