cardiff airport
maes awyr caerdydd

CCTV
Code of Practice

Updated: March 2013

1 Introduction and Objectives

1.1 Introduction

A CCTV (Closed Circuit Television) system has been installed in Cardiff Airport Limited (hereafter referred to as the 'Airport') by Joint Airport, Police and UK Border Force (UKBF) funding. Cardiff Airport's CCTV system comprises approximately 116 cameras. , including fixed/static and pan tilt and zoom (PTZ), providing coverage of the internal (terminal, including baggage make-up areas,) and external (the apron, arriving baggage carousel areas, south side fire section and all Critical Part locations, service/delivery yards, and drop off zones) areas of the airport.

Some cameras are used by Apron Control and Air Traffic Control (ATC) to assist in the efficient management and control of aircraft, apron services, stand allocation, etc. Data recorded from these cameras will, however, be processed in accordance with this Code of Practice.

CCTV images are presented at monitors in the Security Operations Control Room and are recorded digitally. Images are recorded at (minimum) one frame per second throughout the whole 24 hour period.

The CCTV system is linked to South Wales Police/ Wectu and UKBF who maintain secondary monitoring facilities at their CCTV Control Room at Cardiff Airport but do not record images themselves, although they may obtain recordings from the Airport

For the purposes of this document, the 'owner' of the system is Cardiff International Airport Ltd.

For the purposes of the Data Protection Act 1998, the Data Controller is Cardiff International Airport LTD.

Details of key personnel, their responsibilities and contact points are shown at Appendix A.

1.2 Objectives of the System

1.2.1 The Information Commissioner has been notified of the purpose for which the Airport operates CCTV. These are:

Operational Purposes:

Traffic flow and management.
Left or abandoned vehicles.
Air Traffic movement on the ramp, taxiways etc.
Vehicular / other equipment movement on the ramp, taxiways etc.
Passenger flow.
Quality standards management.
Queue management.
Airport and Government regulatory compliance and monitoring.

Safety Purposes:

Public safety.
Employee safety.
Protection of staff and passengers from assault.
To protect staff (eg. Security staff) from allegations of assault or improper behaviour.

Security Purposes:

Passenger movement.
Enforcement of Department for Transport and Home Office security regulations.
Vehicular / equipment movement.
Left luggage.

Law Enforcement Purposes:

Border / Government agency enforcement.
Prevention of crime.
Detection of crime.
Apprehension and prosecution of offenders.
Evidential / court proceedings.

1.22 Within this broad outline, the Managing Director Cardiff Airport LTD, in partnership with South Wales Police, UK Border Force, ICTS has drawn up and published these specific key objectives based on local concerns; they will be reviewed periodically.

1.3 Procedural Manual

A separate Procedural Manual, providing instructions on the operation of the system, supplements this Code of Practice. To ensure the purposes and principles of the CCTV system are realised (see Section 2), the Procedural Manual is based on the contents of the Code of Practice.

2. Statement of Purpose and Principles

2.1 Purpose

The purpose of this document is to state the intention of the owners and managers, on behalf of the partnership as a whole and as far as is reasonably practicable, to support the objectives of the Cardiff Airport CCTV system, and to outline how it is intended to do so.

2.2 General Principles

2.2.1 The CCTV system will be operated fairly, within the law, and only for the purpose for which it was established or which are subsequently agreed in accordance with this Code of Practice.

2.2.2 The CCTV system will be operated with due regard to the rights of the individual, relevant legislation and airport policies and procedures. Particular attention will be paid to the intent of current legislation, e.g. the Data Protection Act, Human Rights Act, Regulation of Investigatory Powers Act, Police and Criminal Evidence Act.

2.2.3 The public interest in the operation of the CCTV system will be recognised by ensuring the security and integrity of operational procedures.

2.2.4 Throughout this Code of Practice it is intended, as far as reasonably possible, to balance the objectives of the CCTV system with the need to safeguard the individual's rights. Every effort has been made throughout the code of Practice to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the CCTV system is not only accountable but is also seen to be accountable.

2.2.5 Participation in the system by an organisation, individual or authority, assumes an agreement by all such parties to comply fully with and be accountable under the Code of Practice.

2.3 Copyright

Copyright and ownership of all material recorded by virtue of the CCTV system will remain with Cardiff International Airport LTD

2.4 Cameras and Area Coverage

2.4.1 The areas covered by CCTV to which this Code of Practice refers comprise the public and private areas, both internal and external, within the responsibility of Cardiff Airport LTD the use of the CCTV system and the data produced by virtue of its use, will always accord with the objectives of the CCTV system.

2.4.2 Some of the cameras offer pan tilt and zoom (PTZ) capability; the others are fixed/static cameras. All cameras provide colour images; some automatically switch to mono-chrome in low light conditions.

2.4.3 None of the cameras forming part of the system will be installed in a covert manner.

2.5 Monitoring and Recording Facilities

2.5.1 The CCTV system is monitored on a 24 hour basis by security staff in the Security Operations Control Room. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period. Recording rates are generally at 1 frame per second; however, as more sophisticated recording equipment is installed, higher frame rates may be achieved.

2.5.2 Secondary monitoring equipment will be located at UKBF Control Offices, WECTU, HSSO. No equipment, other than that housed in the Control Room Equipment Room, shall be capable of recording images from any of the cameras.

2.5.3 The replaying and/or copying of any recorded data will be in accordance with this Code of Practice.

2.6 Unauthorised Access

2.6.1 Unauthorised persons will not have access to the Control Room or Equipment Room without an authorised member of staff being present.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material will be processed and handled strictly in accordance with this Code of Practice and the Procedural Manual.

2.8 Changes to the Code of Practice and Procedural Manual

2.8.1 Any major changes to the code of Practice and/or the Procedural Manual (such as will have a significant impact on the Code of Practice or the operation of the system) will take place only after consultation with, and upon the agreement of all organisations with a participatory role in the operation of the system.

2.8.2 A minor change (such as may be required for clarification and will not have a significant impact on the Code of Practice or the operation of the system) may be agreed between the manager and the owners of the system.

3. Privacy and Data Protection

3.1 Public Concern

3.1.1 Although the majority of the public may have become accustomed to 'being watched', those who do express concern do so mainly over matters pertaining to the processing of the information/data, i.e. what happens to recorded material.

N.B. – 'Processing' means **obtaining, recording or holding** the information/data or **carrying out any operation or set of operations** on the information/data, including:

i. Organisation, adaptation or alteration of the information/data.
ii. Retrieval, consultation or use of the information/data.
iii. Disclosure of the information/data by transmission, dissemination or otherwise making available.

OR

iv. Alignment, combination, blocking, erasure or destruction of the information/data.

3.1.2 All personal data obtained by virtue of the CCTV system shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the system. In processing personal data there will be a total respect for everyone's right to privacy and family life and their home.

3.1.3 Where applicable, cameras will not compromise the privacy of private/residential properties. Where possible, data processing from these cameras will be inhibited, either mechanically or by 'software blanking' to ensure that no data can be obtained from private/residential properties.

3.2 Data Protection Legislation

3.2.1 Operation of the CCTV system has been notified to the Office of the Information Commissioner in accordance with the Data Protection Act 1998, Chapter 29 Part III.

3.2.2 All data will be processed in accordance with the principles of the Data Protection Act which, in summarised form, includes, but is not limited to:

i. All personal data will be obtained and processed fairly and lawfully.
ii. Personal data will be held only for the purposes specified.
iii. Personal data will be used only for the purposes, and disclosed only to the people specified in this Code of Practice.
iv. Only personal data will be held which are adequate, relevant and not excessive in relation to the purposes for which the data are held.
v. Steps will be taken to ensure that personal data are accurate and, where necessary, kept up-to-date.
vi. Personal data will be held for no longer than is necessary.
vii. Individuals will be allowed access to information/data held about them and, where appropriate, permitted to correct or erase it.
viii. Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information/data.

3.3 Requests for Information (Subject Access)

3.3.1 Any request from an individual for the disclosure of personal data that he/she believes is recorded by the CCTV system will be directed to the Data Controller. Appendix E - How to Apply for Access to Information Held on the CCTV System contains guidance and an application form.

N.B. Completed application forms will only be accepted from a solicitor when accompanied by a covering letter. It is the solicitor's responsibility to conduct and document, by means of the application form, the individual's identity check. The individual is responsible for any costs associated with instructing a solicitor.

3.3.2 The principles of the Data Protection Act, Chapter 29, Sections 7 & 8 (Rights of Data Subjects and Others) shall be followed in respect of every request; those Sections are reproduced at Appendix B.

3.4 Exemptions to the Provision of Information

3.4.1 In considering a request made under the provisions of the Data Protection Act, Chapter 29 Section 7, reference may also be made to Section 29(1) which includes, but is not limited to, the following statement:

i. Personal data processed for any of the following purposes;
ii. the prevention or detection of crime;
iii the apprehension or prosecution of offenders;

are exempt from the subject access provisions in any case to the extent to which the applicant of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

N.B. Every application will be assessed on its own merits and general 'blanket exemptions' will not be applied.

3.5 Criminal Procedures and Investigations Act, 1996

The Criminal Procedures and Investigations Act 1996 came in to force in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the presentation of its own case (known as unused material). Disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the Data Controller by Section 7 of the Data Protection Act 1998 (known as subject access).

4. Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, access to the Control Room and Equipment Room is restricted in accordance with this Code of Practice. However, in the interests of openness and accountability, anyone wishing to visit the Control Room and/or Equipment Room may be permitted to do so, subject to the approval of, and after making prior arrangements with the Head of Terminal Services Officer or the Contract Security Manager (ICTS).

4.1.2 Cameras will not be used to look in to private residential properties. 'Privacy zones' and camera end-stops are programmed into the system in order to prevent the interior of any private residential property within range of the system being surveyed by the cameras.

4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the CCTV system may do so by contacting the HTSO.

4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this Code of Practice may be entitled to compensation.

4.2 System Owner

4.2.1 The system owner is Cardiff International Airport LTD, South Wales Police and UKBF.

4.2.2 The Head of Terminal Services & Security Officer, named at Appendix A, being the nominated representative of the System Owner, will have unrestricted personal access to the Control Room and Equipment Room and will be responsible for receiving regular reports from the System Manager and Security Contract Manager (ICTS).

4.2.3 Formal consultation will take place between the owner and the managers of the system with regard to all aspects, including this Code of Practice and the Procedural Manual.

4.3 System Owners Representative

4.3.1 The System Owners Representative will ensure that every complaint is acknowledged in writing within 5 working days. The acknowledgement will include advice to the complainant on the enquiry procedure to be undertaken. A formal report will be forwarded to the nominee of the system owner, named at Appendix A, giving details of all complaints and the outcome of enquiries.

4.4 System Manager

4.4.1 The nominated system manager, named at Appendix A, will have day-to-day responsibility for the system as a whole.

4.4.2 The CCTV system will be subject to audit by the Operations Department at Cardiff Airport and the CCTV User Group, or a nominated deputy whose organisational level is at least equal to that of the System Manager, but who is not the System Manager.

4.5 Public Information

4.5.1 Code of Practice:

A copy of the Code of Practice shall be published on the airport's web-site, and a copy will be made available to anyone on request. Additional copies will be lodged with UKBF, WECTU, Security Contract Manager and Airport Police offices.

4.5.2 Signs:

Signs are located at designated points throughout the Airport.

Signs should be placed so that the Public, Airport Staff and Contractors etc, where appropriate, are aware that they are entering a zone, which is covered by CCTV Surveillance Equipment.

The signs should be clearly visible and legible to members of the public.

The size of the signs will vary according to circumstances e.g:

(a) A sign on the entrance door to a building may only need to be A3 size because the sign is at eye level of those entering the premises whereas,

(b) Signs at the entrances to car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large e.g. A1 size as they are likely to be viewed from a distance. (should CCTV be in operation)

The signs should contain the following information:

(a) Cardiff Airport Limited operates a CCTV system,

(b) The purpose of the CCTV system.

(c) Contact details (telephone number).

An image of a camera should be placed on signs. This is intended to assist individuals who perhaps have learning difficulties etc and to help ensure the lawfulness of CCTV processing of information and images.

5. Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 Periodically, the system will be independently evaluated to establish whether the purposes of the system are being complied with and the objectives are being achieved. The evaluation will incorporate, but will not be limited to, such things as:

a. An assessment of the impact on local crime.
b. An assessment of the impact on airport business ie Security of airport premises, safety of the public, staff and contractors.
c. An assessment of adjacent areas without CCTV (displacement).
d. The views and opinions of the public.
e. The operation of the Code of Practice.
f. Whether the purposes for which the system is established are still relevant.
g. Cost effectiveness and value for money.

5.1.2 The results of the evaluation will be published and, when appropriate, will determine amendments and improvements to the future function, management and operation of the system.

5.1.3 It is intended that evaluations should take place at least every 2 years.

5.2 Monitoring

The Security Contracts Manager will accept day-to-day responsibility for the monitoring, operation and evaluation of the system and the implementation of the Code of Practice.

5.3 Audit

The Operations department audit team of Cardiff Airport, or nominated deputy who is not the System Manager, will be responsible for regular audits of the operation of the system and compliance with the Code of Practice. Audits, which may be in the form of irregular spot-check(s), will include examination of the Control Room, the CCTV recording equipment, the content of recorded material, integrity of log books and documents, etc.

6. Human Resources

6.1 Staffing of the Control Room

6.1.1 The Control Room will be staffed on a 24 hour basis. Equipment associated with the system will only be operated by authorised personnel who have been trained in its use and all Control Room procedures. Each operator will be issued with a personal copy of the Code of Practice and the Procedural Manual; they will be fully conversant with the contents of the Code of Practice and the Procedural Manual, which may be updated from time to time. The will be expected to comply with at all times, as far as is practicable with the CCTV read and sign policy

6.1.2 Airport Police are currently deployed at Cardiff Airport; this 'detachment' liaises closely with airport management and the security section. Police duties which require regular attendance in the Control Room and police officers will:

- Comply with Control Room access and sign the Visitors Book, see section 8.
- Be conversant with the Code of Practice and the Procedural Manual.

6.2 Discipline

6.2.1 Every individual with any responsibility under the terms of the Code of Practice and who has any involvement with the CCTV system will be subject to either;

- Cardiff Airport LTD disciplinary procedures, or
- ICTS Cardiff Airport. disciplinary procedures,

as appropriate. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with these procedures.

6.2.2 The System Owner will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. The Security Manager (ICTS) has day-to-day responsibility for the management of the room and for enforcing discipline. Non-compliance with the Code of Practice by any person will be considered a severe breach of discipline (misconduct) to be dealt with accordingly, including, if appropriate, the instigation of criminal proceedings.

6.3 Declaration of Confidentiality

6.3.1 Every individual with any responsibility under the terms of the Code of Practice and who has any involvement with the CCTV system, will be required to sign a declaration of confidentiality, see Appendix D (also Section 8 concerning access to the Equipment Room). The System Owner and Security Contract Manager will maintain a register of signed declarations of confidentiality.

7. Control and Operation of Cameras

7.1 Guiding Principles

7.1.1 Any person operating the CCTV system will act with utmost probity at all times.

7.1.2 Every use of the cameras will accord with the purposes and objectives of the system and shall comply with the Code of Practice.

7.1.3 Cameras will not be used to look in to private residential properties. Cameras end-stops and 'privacy zones' are programmed in to the system in order to prevent the interior of any private residential property within range of the system being surveyed by the cameras.

7.1.4 Cameras operators will be mindful of exercising prejudices which may lead to complaints of the system being used for purposes other than those for which it is intended. An operator may be required to justify his/her interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the system or by the System Owner or Security Contracts Manager.

7.2 Primary Control

7.2.1 Only those authorised members of staff who receive appropriate training and with responsibility for using the CCTV equipment will have access to the operating controls; those operators have primacy of control at all times.

7.3 Secondary Monitoring

7.3.1 Secondary control monitors are located at :

- Security Control Centre and
- Offices of Designated Airport Security Management.
- Cardiff Airport IT Department for Audit and Fault Issues
- South Wales Police (SB, WECTU)
- UK Border Forces (UK BF)
- Apron Control (Limited Access)
- Air Traffic Control
- NCP
- Fire Section
- Silver Command Suite
- CWL Operations Team

7.4 Operation of the System by the Police

7.4.1 Under exceptional circumstances the police may make a request to assume direct control of the CCTV system. Only formal requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the system owner, or designated deputy of equal standing.

7.4.2 In the event of such a request being granted, the Control Room will continue to be staffed and equipment operated by only those personnel who are authorised and trained to do so and who fall within the terms of Sections 6 and 7 of the Code of Practice.

7.4.3 In very exceptional circumstances, e.g. a major/large scale incident, a request or direction may be made by the police to take total control of the CCTV system, including the staffing of the Control Room. Any such request must be made in the first instance to the System Owner or designated deputy of equally standing. A request for total exclusive control must be made in written by a police officer not below the rank of Assistant Chief Constable or officer of equally standing.

8. Access to and Security of the Control Room and Associated CCTV Equipment

8.1 Authorised Access

8.1.1 Only authorised personnel will operate any of the equipment located within the Control Room and equipment associated with the CCTV system located in the Equipment Room.

8.2 Public Access

8.2.1 Public access to the monitoring and recording facilities will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the System Owner/Security Manager. Any such visits will be conducted and recorded in accordance with paras 8.3 and 8.4.

8.3 Authorised Visits

8.3.1 Visits by inspectors, Control Authorities (CA) or auditors do not fall within the scope of para 8.2 and may take place at any time, without prior warning. No more than 2 inspectors, CA staff or auditors will visit at any one time. Inspectors or auditors will not influence the operation of any part of the CCTV system during their visit. The visit will be suspended in the event of it being operationally inconvenient; any such visit will be recorded in accordance with para 8.4.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, ALL visitors to the Control Room and/or Equipment Room will enter their details and signature in the Visitors Book, thereby indicating their agreement to comply with the Declaration of Confidentiality, see Appendix D.

8.5 Security

8.5.1 Authorised personnel will be present at all times when the equipment is in use. In the event of a Control Room evacuation for safety or security reasons, normal Control Room/terminal procedures will be complied with; no CCTV equipment will be shut down.

9. Management of Recorded Material

9.1 Guiding Principles

9.1.1 For the purposes of this Code of Practice 'recorded material' means any material/data/images recorded by, or as a result of, technical equipment which forms part of the CCTV system; this specifically includes images recorded digitally or by way of copying on to CD-R and 'hard-copy' video prints.

9.1.2 Every recording used in conjunction with the CCTV system has the potential for containing material that has to be admitted in evidence at some point during its life-span.

9.1.3 Members of the community/public must have total confidence that material recorded by virtue of the CCTV system in connection with their routine activities will be treated with due regard to their individual right to respect of their privacy and family life.

9.1.4 It is therefore of the utmost importance that every means of data recording is treated strictly in accordance with the Code of Practice, from the moment it is recorded until it is destroyed/erased. Every movement and usage (processing) will be meticulously recorded.

9.1.5 Access to and use of recorded material will be strictly for the purposes and objectives defined in the Code of Practice.

9.1.6 Recorded material will not be copied, sold, released or used for commercial purposes or for the provision of entertainment.

9.2 National Standards for Access to and Disclosure of Data to a Third Party

9.2.1 All requests for the release of personal data generated by the CCTV system will be channelled through the System Owner who will ensure the principles contained in the Code of Practice Appendix C are applied.

9.2.2 In complying with the National Standards for Access to and Disclosure of Data to a Third Party, it is intended, as far as is reasonably practicable, to safeguard the individual's right to privacy and to give effect to the following principles:

v. Recorded material shall be processed lawfully and fairly, and used only for the purposes and objectives defined in the Code of Practice.
vi. Access to recorded material will only take place in accordance with Appendix C.
vii. The release or disclosure of data for commercial or entertainment purposes is strictly prohibited.

9.2.3 Members of the police service or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C, release details of recorded material to the media only in an effort to identify alleged offenders and/or potential witnesses.

N.B. Release of recorded material to the media, in any format, which may be part of a current investigation, will be covered under the Police and Criminal Evidence Act 1984. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the prosecution and the defence.

9.2.4 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be done in accordance with Appendix C.

9.2.5 It may be beneficial to make use of recorded material for the training and education of those involved in the operation and management of the CCTV system, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of the CCTV system will only be used for such bona-fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3 Retention of Recorded Material

9.3.1 Recorded material will be retained for a maximum period of 30 days this is an approximate number which will vary slightly depending on the capacity of the digital recording units. After this time data will be destroyed / erased by over-writing.

9.4 Recording Policy

9.4.1 Subject to the correct functioning of the recording equipment, images from all cameras will be recorded throughout every 24 hour period, at a minimum of one frame per second, time-lapse mode.

9.5 Evidential Images

9.5.1 In the event of images being required for evidential purposes the details must be entered in to the Evidence Seizure Log in accordance with the Procedural Manual.

Appendix A

Details of Key Personnel and Responsibilities

1 System Owner: Cardiff International Airport Ltd

System Owner's Representative:

Ceri Mashlan
Head of Terminal and Security Operations
Cardiff Airport Ltd
Vale of Glamorgan
CF62 3BD
Tel: 01446 712944
Fax: 01446 712555

Responsibilities:

Cardiff Airport Ltd is the 'owner' of the CCTV system. The Head of Terminal and Security Operations is the single point of reference on behalf of the owner. Her role includes responsibility to:

i. Ensure the provision and maintenance of all equipment forming part of the CCTV system in accordance with contractual arrangements which the owner may from time to time enter in to.
ii. Maintain close liaison with the Security Contract Manager and the System Manager.
iii. Ensure the interests of the owner and other organisations are upheld in accordance with the terms of the Code of Practice.
iv. Agree to any proposed alterations and additions to the system, the Code of Practice and the Procedural Manual.

2 System Manager

Cheryl Bray
Information Systems Support Manager
Cardiff Airport Ltd
Vale of Glamorgan
CF62 3BD
Tel: 01446 712500

Responsibilities:

The Facilities Planner is the System Manager and has delegated authority as Data Controller. Her role includes responsibility to:

i. Maintain functional management of the CCTV system.
ii. In conjunction with the HTSO, develop and amend the Code of Practice and the Procedural Manual.
iii. Liaise with the Security Manager regarding the provision of appropriate CCTV operator training.
iv. Maintain liaison with all operating partners.

3	**Contract Security Manager**	**ICTS Contract Manager** **Airport Security Manager** ICTS Ltd, Cardiff Airport Vale of Glamorgan CF62 3BD Tel: 01446 712509

Responsibilities:

The Security Manager's responsibilities are laid down in the Airport Manual. In respect of the CCTV system, the Security Manager's role includes responsibility to:

i. Maintain day-to-day management of the system (Control Room operators).
ii. Accept overall responsibility for the system and ensure that ICTS staff comply with the Code of Practice and the Procedural Manual.
iii. Liaise with the System Manager regarding requirements for appropriate CCTV operator training.
iv. Maintain liaison with the System Owner and the System Manager.

Appendix B

Extract From the Data Protection Act 1998

Chapter 29 Part II, Sections 7 and 8

Section 7 – Right of access to personal data.

(1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled –

(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,

(b) if that is the case, to be given by the data controller a description of –

I. the personal data of which that individual is the data subject,
II. the purpose they are being or are to be processed, and
III. the recipients or classes of recipients to whom they are or may be disclosed,

(c) to have communicated to him in an intelligible form –

I. the information constituting any personal data of which that individual is the data subject, and
II. any information available to the data controller as to the source of those data, and

(d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly effecting him, to be informed by the data controller of the logic involved in that decision-taking.

(2) A data controller is not obliged to supply any information under subsection (1) unless he has received -

(a) a request in writing, and

(b) Except in prescribed cases, such fee (not exceeding a prescribed maximum) as he may require.

(3) A data controller is not obliged to comply with a request under this section unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks.

(4) Where a data controller cannot comply with a request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless –

(a) the other individual has consented to the disclosure of the information to the person making the request, or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(6) In determining the purposes of subsection (4)(b) whether it is reasonable in all circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to -

(a) any duty of confidentiality owed to the other individual,

(b) any steps taken by the data controller with a view to seeking the consent of the other individual,

(c) whether the individual is capable of giving consent, and

(d) any express refusal of consent by the other individual.

(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his request is limited to personal data of any prescribed description.

(8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9) If a court is satisfied on the application of any person who has made a request under the foregoing provisions of this section that the data controller in question has failed to comply with the request in contravention of these provisions, the court may order him to comply with the request.

(10) In this section -

"prescribed" means prescribed by the Secretary of State by regulations;

"the prescribed maximum" means such amount as may be prescribed;

"the prescribed period" means the forty days or such other period as may be prescribed;

"the relevant day", in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).

(11) Different amounts of periods may be prescribed under this section in relation to different cases.

Section 8 – Provision Supplementary to Section 7

(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under the provisions of that subsection.

(2) The obligation imposed by section (7). (c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless -

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(c) the data subject agrees otherwise; and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent request under that section by that individual unless a reasonable interval has elapsed between compliance with a previous request and the making of the current request.

(4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regards shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(5) Section 7(1).(d) is not to be regarded as requiring the provision of information as to the logic involved in any decision-taking if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to a request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(7) For the purposes of section 7(4) and 7(5) another individual can be identified from the information being disclosed if he can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Appendix C

Access to and Disclosure of Data to Third Parties

Control of Data/Images

Access to and disclosure of images recorded by the CCTV system must be restricted and carefully controlled for 2 main reasons:

a. To ensure that the rights of individuals are preserved.
b. To ensure that the chain of evidence remains intact should the images be required for evidential purposes.

Principles of Access and Disclosure

Access to and disclosure of recorded images should only be made to authorised agents in the following circumstances:

- Law enforcement agencies; where the recorded images would assist in a specific criminal enquiry.
- Prosecution agencies.
- Relevant legal representatives.
- The media; where it is agreed that the public's assistance is needed in order to assist in the identification of a perpetrator, victim, or witness in relation to a criminal incident.
- People whose images have been recorded and retained, unless this would prejudice criminal enquiries/proceedings.

N.B. No recorded material is to be released to the media without the specific permission of the System Owner Head of Terminal Services and Security Operations or the Operations Director.

Requests for Access to Images

All requests for access to and disclosure of images shall be recorded in the Request for footage log and/or the Evidence Seizure Log as appropriate. In some circumstances it may also be appropriate to record the details in the Control Room Occurrence Log. An entry must contain full details of the time and date of the incident, name of the person making the request, the request itself, and their reasons.

If access/disclosure is refused, the reason shall be entered in to the Log(s).

If access/disclosure is granted then the following shall be entered in the Log(s):

i. The date and time at which access was allowed or disclosure made.
ii. Details of any 3rd party who was allowed access or to whom disclosure was made.
iii. The reason(s) for allowing access/disclosure.
iv. The extent of the information to which access/disclosure was allowed (camera numbers, dates, times, etc).

Appendix D

Declaration of Confidentiality

The following pages contain examples of 'Declaration of Confidentiality' forms applicable to:

- Airport employees (CCTV operators).
- CCTV system inspectors and auditors.
- Authorised visitors.

Copies of the Declaration of Confidentiality are;

- displayed on the door if the Control Room, and
- held in the Visitors Book (laminated copy).

All members of staff must comply with the Declaration of Confidentiality. All visitors must sign the Visitors Book, thereby indicating that they have read, understood and will comply with the Declaration of Confidentiality.

Declaration of Confidentiality

Airport Employee (CCTV Operators)

I am employed by …….to perform the duties of CCTV Operator at Cardiff Airport. I have received a copy of the Code of Practice for the operation and management of the CCTV system.

I hereby declare that:

I am fully conversant with the content of the Code of Practice and I understand that all duties that I undertake in connection with the Cardiff Airport CCTV system must not contravene any part of the current Code of Practice or any future amendments. If now, or in the future, I am or become unclear on any aspect of the operation of the system or the content of the Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my duties in connection with the Cardiff Airport CCTV system, verbally, in writing or by any other media, now or in the future, including such time as I may no longer be employed in connection with the CCTV system.

In signing this declaration, I agree to abide by the Code of Practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format, now and in the future.

Signed:…… Print Name:……..

Position:……

Witness:……..

Dated the…….day of…….20…..

Declaration of Confidentiality

CCTV System Inspectors and Auditors

I am a voluntary inspector/auditor of the Cardiff Airport CCTV system with a responsibility to monitor the operation of the system and adherence to the Code of Practice. I have received a copy of the Code of Practice for the operation and management of the CCTV system.

I hereby declare that:

I am fully conversant with my voluntary duties and the content of the Code of Practice. I undertake to inform the System Owner and/or the System Manager of any apparent contravention(s) of the Code of Practice that I may note during the course of my visits to the monitoring facility.

If now, or in the future, I am or become unclear on any aspect of the operation of the system or the content of the Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my voluntary duties that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my duties in connection with the Cardiff Airport CCTV system, verbally, in writing or by any other media, now or in the future, including such time as I may no longer be performing the role of CCTV system inspector/auditor.

In signing this declaration, I agree to abide by the Code of Practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format, now and in the future.

Signed:…… Print Name:……..

Position:……

Witness:……..

Dated the…….day of…….20…..

Declaration of Confidentiality

Authorised Visitor

I am an authorised visitor to the Cardiff Airport Control Room and CCTV system.

I hereby declare that:

I understand that it is a condition of my visit that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my visit in connection with the Cardiff Airport CCTV system, verbally, in writing or by any other media, now or in the future.

In signing this declaration, I agree to maintain confidentiality in respect of all information gained during the course of my visit, whether received verbally, in writing or any other media format, now and in the future.

Signed:…… Print Name:……..

Position:……

Witness:……..

Dated the…….day of…….20…..

Appendix E

How to Apply For Access to Information Held On the Cardiff Airport CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. Cardiff Airport will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Airport is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

The Airport's Rights

Cardiff Airport may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, Postal Orders, etc. should be made payable to **'Cardiff Airport Ltd.**

THE APPLICATION FORM:

(N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)

Section 1 Asks you to give information about yourself that will help the Airport to confirm your identity. The Airport has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full face photograph of you.

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 **You must sign the declaration**

When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to:

THE CCTV SYSTEM MANAGER, Cardiff Airport Ltd, CF62 3BD

If you have any queries regarding this form, or your application,
please ring the CCTV System Manager on 01446 711111

SECTION 1 About Yourself

The information requested below is to help the Airport (a) satisfy itself as to your identity and (b) find any data held about you.

PLEASE USE BLOCK LETTERS

Title *(tick box as appropriate)*	Mr		Mrs		Miss		Ms	
Other title *(e.g. Dr., Rev., etc.)*								
Surname/family name								
First names								
Maiden name/former names								
Sex *(tick box)*	Male				Female			
Height								
Date of Birth								
Place of Birth	Town							
	County							
Your Current Home Address *(to which we will reply)*								
	Post Code							
A telephone number will be helpful in case you need to be contacted.	Tel. No.							

If you have lived at the above address for less than 10 years, please give your previous addresses for the period:

Previous address(es)		
Dates of occupancy	From:	To:
Dates of occupancy	From:	To:

SECTION 2 Proof of Identity

To help establish your identity your application must be accompanied by **TWO** official documents that between them clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving license, medical card, passport or other official document that shows your name and address.

Also a recent, full face photograph of yourself.

Failure to provide this proof of identity may delay your application.

SECTION 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to?

(a) View the information and receive a permanent copy YES / NO

(b) Only view the information YES / NO

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by | Date

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

NOW – please complete Section 5 and then check the 'CHECK' box before returning the form.

SECTION 5 To Help us Find the Information

If the information you have requested refers to a specific offence or incident, please complete this Section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.

If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.

Were you: *(tick box below)*

A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	
Other – please explain	

Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident	

Before returning this form - Have you completed **ALL** Sections in this form?

Please check: Have you enclosed TWO identification documents and a recent photograph of yourself?
Have you signed and dated the form?
Have you enclosed the £10.00 (ten pound) fee?

Further Information:

These notes are only a guide. The law is set out in the Data Protection Act, 1998, obtainable from The Stationery Office. Further information and advice may be obtained from:

The Information Commissioner,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.
Tel. 0303 123 1113

Please note that this application for access to information must be made direct to **Cardiff Airport Ltd** (address on page 2) and **NOT** to The Information Commissioner.

OFFICIAL USE ONLY

Please complete ALL of this Section (refer to 'CHECK' box above).

Application checked and legible? ☐

Identification documents checked? ☐

Details of 2 Documents (see page 3)

Date Application Received

Fee Paid

Method of Pa

Receipt No.

Documents Returned?

Member of Staff completing this Section:

Name

Location

Signature

Date

Appendix F

CCTV Monitoring Information Signs

The following page contains the CCTV monitoring information sign displayed at Cardiff Airport;

i. at the entrances to the terminal building, landside and airside;
ii. in the car parking areas;
iii. at the entrances to the airport.

The design and location of these signs are chosen to be compliant with the Data Protection Act 1998.

Other signs relating to CCTV surveillance are located around the airport and the car parking areas; these signs are for the purposes of;

i. providing information to passengers and the public, and
ii. the deterrence of crime.

There is no requirement for these additional signs to be compliant with the Data Protection Act 1998.

WARNING

Recorded CCTV cameras are in operation throughout the airport for operational, safety, security, and law enforcement purposes.

This scheme is operated by Cardiff Airport.
For further information please contact 01446 711111.

RHYBUDD

Mae camerâu teledu cylch cyfyng sy'n recordio ar waith ym mhob man yn y maes awyr at ddibenion gweithredol, diogelwch, a gorfodi'r gyfraith.

Mae'r cynllun hwn yn cael ei weithredu gan Faes Awyr Caerdydd.
Am ragor o wybodaeth cysylltwch â 01446 711111.

Notes:

Notes: