Driving Standards Agency
CCTV Policy

Author – redacted section 40

Title:	CCTV Policy
Classification:	Not protectively marked
Descriptor:	Policy
Policy Reference:	POL/46/11
Summary:	Policy on how the Driving Standards Agency (DSA) uses CCTV in compliance with legislation and relevant guidance
Status:	Initial Draft
Version No:	1.0
Date Approved:	October 2010
Date of Review:	13 February 2012
Originator:	Information Assurance Support Officer
Policy Owner:	Knowledge and Information Manager
Who to contact for queries:	DSA Knowledge & Information Management Team
Related Policies and Guidance	• ICO's CCTV Code of Practice • DSA Data Protection Policy • DSA Records Management Policy • DSA ICT Disposal Policy
Audience:	All DSA staff involved with the use of CCTV and SARs and any associated relevant 3rd parties
Reference	• CCTV Policy – Mersey Care NHS • CCTV Policy – South Devon NHS • CCTV System Policy - Bassinbourn Community Primary School • Closed Circuit Television Policy – 5 Boroughs Partnership NHS • Closed Circuit Television Policy – West Lincolnshire NHS • Closed Circuit Television Policy – Brunel University • CCTV Code of Practice - ICO

Issue Number	Date	Issued By	Reason for Issue	Issued to
0.0.1	19 Feb 09	Redacted section 40	Reviewed Draft	IA Branch
0.0.1	24 Feb 09		Comments response	IA Branch, PCS
0.0.2	10 Dec 09		Reviewed draft	IA Branch, Facilities Notts
0.0.3	17 Feb 10		Review of Draft	IA Branch, Area contacts
0.0.4	29 Mar 10		Review of changes	IA Branch
0.0.5	5 Jul 10		For review and clearance.	IA Branch, PCS, Diversity Groups
1.0	Oct 10		Approval for publication	Head of IA
1.0	13 Feb 12		Annual review	N/A

CONTENTS

INTRODUCTION

This policy outlines the use of Closed Circuit Television (CCTV) systems within DSA Estates and should be read in conjunction with the DSA Data Protection Policy.

1. POLICY OBJECTIVES

1.1 The objectives for this policy are to:

1.1.1 Ensure the DSA installs and uses CCTV systems correctly in a fair and lawful manner so that the systems cannot be misused or abused.

1.1.2 Ensure that the DSA are compliant with relevant legislation which includes but is not restricted to:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Official Secrets Act 1989
- The Regulation of Investigatory Powers Act 2000

1.1.3 All contactors who have installed and/or are operating CCTV systems on behalf of the DSA must adhere to this Policy.

1.2 The following acts/guidance have been taken into account when drafting this policy:

- The Data Protection Act 1998
- The CCTV Code of Practice (Revised Edition) produced by the Information Commissioner
- Human Rights Act 1998
- The Official Secrets Act 1989
- The Regulation of Investigatory Powers Act 2000
- DSA Information Security Policy
- DSA Data Protection Policy
- Privacy Impact Assessment (PIA) template and guidance

1.3 This policy should be read in conjunction with the following DSA Policies and SOPs:

- DSA CCTV SOP
- DSA Data Protection Policy
- DSA Information Security Policy

- DSA Incident Management Policy
- DSA SAR SOP
- DSA FOI SOP
- DSA Staff Handbook
- DSA Safety Policy
- Privacy Impact Assessment (PIA) template and guidance
- DSA Information Charter

1.4 The designated owner for each DSA or third party site is:

- Headquarters – HEO Facilities Manager Nottingham
- Cardington – Sodexo Contract Manager
- Driving Test Centres North – ODM North
- Driving Test Centres South- ODM South
- Theory Test Centres – Theory Test Contract Manager

2. PURPOSE

2.1 This policy covers all staff working in the Driving Standards Agency and associated employees of any third parties/delivery partners.

2.2 The purposes of using CCTV within the DSA are:

- Assist in the prevention and detection of crime
- Assist with the identification, apprehension and prosecution of offenders
- Safeguard staff with regards to criminal incidents
- Monitor security of DSA-occupied sites

2.3 No CCTV system should be initiated, installed or moved without a Privacy Impact Assessment being carried out and any SOP requirements being met.

2.4 For security and the prevention and detection of crime, CCTV systems may be operated 24 hours a day.

2.5 All schemes will be operated with due regard for the privacy of all individuals at all times and CCTV systems will only be used for the purposes that they are installed for.

3. CAMERAS

3.1 Cameras must be adequate for the purpose for which they have been installed and must be regularly maintained in line with manufacturer's guidance to remain in good working order and to ensure clear images are recorded. Cameras must not be hidden from view.

3.2 The DSA must make every effort to position cameras so they only cover DSA premises. Cameras must not be repositioned to view areas outside of DSA property boundaries without a Privacy Impact Assessment being carried out.

3.3 Existing and new Camera's should be set up so that sound recording is not possible.

3.4 The DSA must clearly display signs so that staff, visitors and members of the public know they are entering an area covered by CCTV. These signs must also indicate the purpose of the system and contact details of the operator of the system in line with guidance from the Information Commissioners Office.

3.5 Only for specifically defined instances, as outlined in the relevant area of the DSA CCTV SOP, and in accordance with the declared purposes and objectives of this policy, may surveillance equipment be used for targeted observation. The Regulation of Investigatory Powers Act 2000 regulates the use of covert/directed surveillance of this type. Use of CCTV in these instances is only permissible when authorised in accordance with these regulations.

4. IMAGES

4.1 Images produced by CCTV must be as clear as possible so they are effective for the purposes they are intended for.

4.2 Cameras and signs must be checked at a minimum annually or, if required, more frequently to ensure that they are adequate as outlined in the relevant DSA CCTV SOP.

4.3 Suitable equipment must be used to ensure that third party information on CCTV images can be anonymised as outlined in the relevant DSA CCTV SOP.

5. RETENTION

5.1 CCTV retention periods must be agreed in accordance with the DSA's Records Management Policy and documented within the DSA Retention schedule in accordance with the CCTV SOP.

5.2 Images may need to be kept for a longer period than outlined in the retention schedule if needed by a third party as identified at paragraph 7.1. All suitable measures to ensure security and integrity of the media must be followed as outlined in the relevant CCTV SOP. Where such a need is known, recordings must not be overwritten.

5.3 All information must be subject to controlled disposal as outlined in DSA Policies including ICT Disposal Policy and the Security Policy Framework (SPF).

6. ACCESS

6.1 Under the Data Protection Act 1998 individuals have the right to request personal information about themselves which includes CCTV images. All requests for information must be dealt with in accordance with the DSA SAR SOP and Data Protection Policy.

6.2 Images can only be disclosed in accordance with the purpose(s) that they were originally collected for or, in accordance with legislative requirements, as outlined in the DSA Data Protection Policy.

6.3 Recorded images and media must be stored and viewed in a secure, restricted area with restricted staff access.

6.4 Any media being viewed or any further processing must be logged in accordance with the relevant DSA CCTV SOP. Any DSA or third party staff involved with handling the CCTV system for this type of processing must have appropriate training.

6.5 Access to CCTV control rooms, or if recorded media is stored on a network, access to that area of the network, must be restricted at all times as outlined in the DSA CCTV SOP.

7. DISCLOSURE

7.1 Any disclosures of any information to any parties must be made in accordance with the guidelines set out in the DSA Data Protection Policy.

7.2 Information required to be disclosed must be released in accordance with the DSA CCTV SOP. All processing of information must be logged in accordance with the DSA CCTV Policy. Data will be disclosed in line with relevant legislative/regulatory requirements.

7.3 Any requests for disclosure of information must be dealt with in accordance with the Data Protection Act. The DSA will provide relevant SOP's for this.

8. MAINTENANCE

8.1 Non Digital systems

8.1.1 A comprehensive log must be kept which records all adjustments/alterations/services/non availability of all CCTV schemes.

8.1.2 Tapes on which images have been recorded on must be replaced once used 12 consecutive times. The image quality of the tapes must be checked regularly as outlined in the DSA CCTV SOP. Once a tape has been used 12 consecutive times, it must be erased and disposed of in a secure manner as outlined in the DSA CCTV SOP and the DSA ICT Disposal Policy.

8.1.3 The record of location/time/date as well as the images recorded will be checked weekly for accuracy and adjusted accordingly, to ensure that images are being correctly recorded. Alterations due to 'British Summer Time' must be checked for accuracy.

8.1.4 A separate log for when and who changes tapes must be kept.

8.1.5 Annual (or more frequent) reviews to assess use against the purpose of the CCTV system must be completed as outlined in the DSA CCTV SOP

8.1.6 All sites must hold a suitable minimum stock of blank tapes for use in the recording device.

8.2 Digital systems

8.2.1 A comprehensive log must be kept which records all adjustments/ alterations/ services/ non-availability of all CCTV schemes.

8.2.2 The record of location/time/date as well as the images recorded will be checked weekly for accuracy and adjusted accordingly, to ensure that images are being correctly recorded. Alterations due to 'British Summer Time' must be checked for accuracy.

8.2.3 Any Digital CCTV system must have appropriate storage space for recording as outlined in the DSA CCTV SOP.

8.2.4 Sites where digital CCTV systems are installed must have access to a recording device that is compatible with the system in use. If applicable, a playback device that is compatible with the system must also be used.

8.2.5 All sites must hold a suitable minimum stock of blank, write once, media for use in the recording device as outlined in the relevant DSA CCTV SOP.

9. SCOPE

9.1 Applies to all staff working in the DSA and associated third parties that have access to CCTV systems.

9.2 Third parties acting on behalf of the DSA installing or running CCTV systems must have a contract/agreement that includes clauses relating to compliance with this policy.

10. ROLES AND RESPONSIBILITIES

10.1 This policy is owned by the Knowledge and Information Manager. The Knowledge and Information Management Team (K&IM) based in DSA's Information Assurance Branch will carry out periodic reviews of this policy, recommending amendments and variations as appropriate.

10.2 It is the responsibility of all staff, including temporary staff and contractors, to be aware of this policy and its requirements.

10.3 To support staff, DSA will make available further specific information in the form of Standard Operating Procedures (SOP); DSA will also make available specific background information to staff on the DSA Intranet. This information will include, but will not be limited to, associated DSA policies and procedures in addition to guidance on the relevant legislation.

10.4 Whilst DSA controls and is responsible for information held in its name, individual members of staff and external contractors should be aware of their personal responsibility and obligations; relevant Information Asset Owners

(IAOs), however, must assume overall responsibility for ensuring that all data, information and records for which they are responsible are managed correctly, appropriately and in compliance with relevant legislation, codes of practice and guidance.

11. SANCTIONS AND VIOLATION

11.1 Breaches of this policy may result in disciplinary action as outlined in the DSA Staff Handbook.

11.2 All complaints must be investigated promptly and thoroughly as outlined in the DSA CCTV SOP. Serious breaches must be investigated independently and reported to the Information Commissioners Office (ICO) as set out in the DSA Incident Management Policy. More information on Serious Breaches can be found in the ICO's guidance, Notification of Data Security Breaches to the Information Commissioner's Office can be found on the ICO website.

12. REVISIONS AND REVIEW

12.1 This policy will be reviewed annually and every time a Privacy Impact Assessment indicates a possible change to the Policy.

13. DEFINITIONS AND GLOSSARY

Personal Data – data which relates to a living individual who can be identified:

- From the data or
- From the data and other information which is in the possession of, or is likely to come into the possession of the data controller

Data Controller - a person or organisation who (either alone or jointly in common with other persons/organisations) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Processing – means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data which includes:

- Organisation, adaptation or alteration of the information or data
- Retrieval, consultation or use of the information or data
- Disclosure of the information or data by transmission, dissemination or otherwise making available

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

CCTV system/CCTV Scheme – the use of video cameras in a closed circuit or network that transmits information to a specific location or monitor.