

Royal Mail Internal Information

RM LETTERS - CODE OF PRACTICE:

USE OF CCTV & DISCLOSURE OF CCTV IMAGES

Final Version

Compilation Date: 6th June 2008

Review Date: 6th June 2009

Tony Marsh

Security General Manager

Royal Mail Security

Mobex 5367 2681

Mobile 07809 756 682

Contents

Rationale.....	3
Basic Principles.....	3
Code of Practice.....	3
Supporting Documents.....	4
Change Control.....	5
Authorisation.....	5
Distribution List.....	5
Document History.....	5
Document Change History.....	5
Glossary.....	5

Rationale

This document is designed to give guidance to users of Closed Circuit Television (CCTV) in respect of data captured by them in the form of images.

Legislation such as the Data Protection Act, Business Standards, and agreements with interested parties such as the CWU, all impact on when and how this data can be used and disclosed.

Basic Principles

RML has a prime responsibility for developing and maintaining a secure environment protecting business assets, including its customer's property and its employees. It is accepted that installation of electronic security systems forms an integral part of the RML security strategy and uses developing technology to best commercial advantage.

The primary purposes of CCTV systems are site management, crime prevention, and crime detection through investigations led by RML Security Managers.

With the advent of increased storage capability such as Digital Video Recorders (DVR's), systems are increasingly likely to record 24hrs a day wherever possible, but are not universally deployed at this time.

RML reserves the right to use images as evidence in the investigation of criminal activity, serious accidents or serious misconduct which has put employees' security/health and safety at risk.

The use of images as evidence gained by this means for criminal investigations will be subject to the strict legal rules of evidence in force at that time.

Due to the increased use of electronic security systems for both security and general site management, RML Security and the CWU has reviewed the previous Guidelines and established the following agreed Code of Practice. Responsibility for conformance with the Code of Practice rests with the users of all CCTV systems.

All enquiries over the application of the Code should be referred to the local Security Manager in the first instance.

Code of Practice - For the Use of CCTV & Disclosure of images obtained from CCTV systems

This Code of Practice applies equally to new and existing buildings/sites.

General

CCTV systems are not to be used by Operational Managers to monitor the general conduct or performance of staff in normal pursuance of their duties.

CCTV may be set for routine continual video recording.

Images captured by any CCTV system will only be analysed or used by RML Security. The only exception to this would be where a serious accident has occurred or where a serious act of misconduct is identified and employees security or health and safety has been put at risk e.g. criminal damage, reckless driving, blocking of a fire exit. In these instances there will be no responsible alternatives other than to analyse/use any relevant images captured or seen.

Requests for the release/use of images or recordings by users or managers other than RML Security must be submitted through the National Physical Security Manager or deputy for consideration and endorsement where they agree release is appropriate.

Crime Prevention/Detection

RML Security may use any system for direct observation or analysis when criminal activity is known or suspected, ensuring compliance with all current legislation and business standards.

CCTV may be used as a crime prevention measure to assist access control, intruder confirmation, perimeter protection, or to monitor high value operations or installations such as safes and strong rooms.

Operational managers or supervisors will not be given access to, or the use of investigative CCTV systems for normal pursuance of operational duties.

Access/Site Security

Where CCTV is installed to provide access control, site security, and perimeter protection, monitors will be manned/watched at all times by Gatekeepers/Doorkeepers or Reception duties as appropriate.

25th June 2008

Use of CCTV & Disclosure of CCTV Images

Code of Practice

RML has a prime responsibility for maintaining a secure environment, protecting business assets, customer's property and its employees. It is therefore accepted that installation of electronic security systems now forms an integral part in this.

RML Security and the CWU have therefore reviewed the previous Guidelines and established a new agreed Code of Practice, which is now published on the Intranet. In addition you will also find the following supporting documents:

Access Control Management Procedure

Closed Circuit Television (CCTV) Management Procedure

Intruder Alarm Management Procedure

The Code of Practice makes it clear that the primary purpose of images such as from CCTV systems is to assist in the detection of crime and safeguard RML assets and our customers' property. It is not a tool for the routine monitoring of the behaviour or performance of staff in normal pursuance of their duties.

It also makes it clear that the image data captured by CCTV systems will only be analysed and used by RML Security unless exceptionally there is a requirement to investigate into the cause of a serious accident or matter of serious misconduct which has put employees' security or health and safety at risk.

Requests for the release/use of images or recordings by users or managers other than RML Security must be submitted through the National Physical Security Manager or Deputy for consideration and endorsement where they agree release is appropriate.

All enquiries over the application of the Code should be referred to the local Security Manager in the first instance.

Tony Marsh

RML Security

Martin Collins

CWU