CCTV Policy

1.0 INTRODUCTION

1.1 CCTV systems installed in EYMS Group vehicles and premises are intended to:

- Provide a safer environment for staff, customers and members of the public on buses, in stations and in depots.
- Deter prospective offenders.
- Assist in determining the cause and severity of accidents to assist in insurance claims.
- Lessen the costs associated with vandalism to properties and vehicles.
- Assist in preventing fraud by drivers and customers.
- Provide recordings under strictly regulated conditions to permit detection and identification of offenders.

1.2 This Code of Practice is designed to:

- Ensure that the CCTV System achieves its purpose with fairness and sensitivity.

1.3 The owner of these systems is:

- EYMS Group Limited, 252 Anlaby Road, Hull, HU3 2RS.

1.4 The areas covered and the equipment specification are:

- As detailed in the Operating and Maintenance Manuals supplied with the systems employed in the various locations.
- Any depot/vehicle at any location where EYMS or its subsidiaries may operate from.

1.5 Copyright:

- EYMS Group Ltd retains the copyright to images recorded and on any stills photographs produced from monitors operated by digital recording equipment recorded by this scheme. No image obtained from monitoring or recording activity can be reproduced by any organisation or by any individual without the express permission of the Data Protection Officer.

1.6 The System Manager is:

- W B Marsden, Data Protection Officer, EYMS Group Limited, 252 Anlaby Road, Hull, HU3 2RS.

1.7 The System Operators are:

- As designated by the Data Protection Officer but no more than two per depot location and any bus/vehicle owned by the group.

1.8 All job name descriptions and equipment descriptions are noted in Appendix 1

2.0 DATA PROTECTION IMPLICATIONS

2.1 The System is:

- Registered with the Information Commissioners Office

3.0 CHANGES TO THE CODE

3.1 Changes to the Code can only be made by:

- Executive Officer/Director/Data Protection Officer.

4.0 MANAGEMENT OF THE SYSTEM

4.1 Overall responsibility for the CCTV scheme

- Lies with the Data Protection Officer.

4.2 The Data Protection Officer will arrange the following:

- Designate day to day responsibility to staff.
- Devise detailed operational guidelines and review operational arrangements and revise the Code of Practice where appropriate.
- Discuss any complaints from the public about operation of the system and take appropriate action.
- Designate persons to review the recorded digital images and tapes.
- Designate persons to remove recording discs for evidential purposes.
- Ensure that privacy is respected, and
- Ensure that requirements of the Data Protection Act are met.

5.0 PUBLIC INFORMATION

5.1 Camera Positioning:

- All areas that may be covered by cameras have appropriate notification signs advising of the existence of CCTV and the identity of the owner of the system.

5.2 A copy of this Code of Practice is available from:

- Data Protection Officer, EYMS Group Limited, 252 Anlaby Road, Hull, HU3 2RS.

6.0 INDIVIDUAL RIGHTS

6.1 Individual privacy:

- Must be appropriately safeguarded and given due regard.
- Private and family life and the home must be respected.
- Cameras must not be used to look into private property. Private residences may come into view only as part of a wide angle or long shot, or as a camera is panning past them, or a camera on a vehicle is driving past them.
- Tracking and monitoring of individuals must be justifiable.
- Must be considered in the operation of any system, in accordance with the relevant section of the Human Rights Act 1998 Individual Rights.

7.0 ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

7.1 The system shall be evaluated by the Data Protection Officer:

- To ensure that the purposes for which the system was established are being maintained.
- To ensure that the monitoring complies with the Code of Practice. This shall include carrying out an audit of the system including examination of records, disc histories and the content of recorded discs.

8.0 STAFF

8.1 Operators of CCTV:

- Shall be designated by the Data Protection Officer.

8.2 Staff training shall be provided :

- By the Data Protection Officer and/or another qualified individual authorised by the DPO and system suppliers when necessary.

8.3 Staff shall be required to:

- Maintain high standards of probity and confidentiality.
- Acknowledge receipt and understanding of this code of practice.
- Ensure proper use of the equipment or recordings. Any abuse or improper use may be the subject of disciplinary hearings.

9.0 COMPLAINTS

9.1 About the operator of the system from the public or others:

- Will be dealt with by the Data Protection Officer who will investigate the complaint and take the appropriate action in the event of any breach of this Code of Practice. This may lead to disciplinary proceedings.

9.2 A member of the public may also complain:

- To the Information Commissioners Office.

10.0 CONTROLS AND OPERATION OF CAMERAS

10.1 Operating Controls:

- Only staff with responsibility for using the equipment shall have access to operating controls.

10.2 Viewing:

- Cameras must not be used to look into private property or into sensitive areas concerning personal privacy.

10.3 Checking:

- Spot checks will be carried out to ensure compliance with the previous items and operators are aware that recordings are subject to routine audit and they may be required to justify their interest to a member of public or a particular property.

11.0 ACCESS TO AND SECURITY OF MONITORS/EQUIPMENT

11.1 Access to view monitors and/or to operate equipment:

- Shall be limited to the designated operators of the systems, the Data Protection Officer or designated staff and the Police.

11.2 Public access to or demonstration of monitors shall not be allowed, except:

- Where a demonstration is provided to an individual to reassure that a particular camera does not view into their private residence other than on an incidental basis
- Where recorded data is shown to the subject/s and they can provide a just cause, in writing, and the Data Protection Officer approves such request.

12.0 RECORDED MATERIAL

12.1 Register Storage:

- The data register must be stored in a secure cabinet or locked safe room and kept locked at all times when unattended.

12.2 Data Usage:

- Digital systems will have their hard drive left in the recording device and set to record a minimum of 10 days on a rolling basis. These will only be removed for necessary viewing of incidents and maintenance.

12.3 Data required for evidential purposes:

- Must be separately indexed and securely stored to avoid accidental use.

12.4 Disposal of data:

- The Data Protection Officer shall ensure the secure disposal or destruction of data when appropriate.

12.5 Labelling:

- Data and hard drives to be individually and uniquely identified and labelled by the Operator.

12.6 Suspicious Incidents:

- Where Police have reasonable grounds for believing that a suspicious incident has been recorded, a Police Officer will arrange to view the data or a copy on CD of a digital recording by contacting the DPO. The Police may remove the data from EYMS as evidence as part of their investigation provided it is agreed by the DPO. This would normally be given except where it may incriminate EYMS Group Ltd. In which case it should be ordered through the normal judicial process. The Data Protection Officer and the Police Officer will log all removals of such data in the data register.

12.7 Data Removal:

- Once the data has been removed by the Police Officer, the Police will assume full responsibility for its security and integrity as evidence to be produced in court.

12.8 Copy Discs:

- No copies of data will be made without the express permission of the Data Protection Officer.
- Copies shall not be made other than for the prevention or detection of crime, for the presentation of evidence in court or for access by the defence in accordance with the Data Protection Act. Or investigation by an insurance company.

12.9 Data Management:

- All data should be kept in a locked cabinet when unattended and data should not be stored without the cabinet. Access to the digital recording equipment on bus should be locked at all times, with only nominated people holding keys.

13.0 DEALING WITH INCIDENTS

13.1 Incidents which require Police investigation:

- Shall be referred to the local Police Station where designated local contacts will form a working relationship with the system administrator.

Appendix 1

Within the policy descriptions are used of equipment and descriptions of persons. These are listed below.

Executive Officer is an officer of the company who holds the power of an executive decision for example Director, Chief Executive or Chairman.

Data Protection Officer is the person who oversees the policy and administration of the policy within the EYMS Group Ltd.

System Manager is the person who controls the workings of the actual CCTV systems and includes their maintenance, repair and renewal.

System Operators are the companies under the control of the Data Protection Officer.

Discs are the medium used in the transfer of data from the on bus system. This is usually CD-ROM but can be DVD or memory stick.

APPENDIX 2

1. The managers authorised to view the data are (by position):-
   DM-H, DM-SC, SI, TM-F, MD-W, D-F, DPO, GPM.

2. The persons authorised to download data are (by position):-
   DT-EY, Ass DT-EY, ATM-F,

3. The persons authorised to maintain the data systems are (by position):-
   DT-EY, Ass DT-EY, FE-F who also authorises the persons he controls at Finglands and Whittles.

4. The equipment authorised by the DPO is either on bus or in depots at company locations. The systems are all-digital and comply with the above noted policy.