



South Yorkshire Fire & Rescue

WORKING FOR A SAFER SOUTH YORKSHIRE

South Yorkshire Fire and Rescue Authority CCTV Scheme

Document History

Version Control

| Version Number | Date | Author | Description | Review Date |
|----------------|--------|--------|-------------------------------|-------------|
| V 1.0 | .09.06 | | Initial Document | |
| V 2.0 | .11.06 | | CCTV Trial Version | |
| V 3.0 | .03.07 | | System Implementation Version | 03.09 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Changes made will require approval from one or all of the persons listed below dependent on the degree and impact of the change.

Approved by:

Data Protection Officer

Date

| | |
|--|--|
| | |
|--|--|

Disclosure Officer

Date

| | |
|--|--|
| | |
|--|--|

Index

| <u>SECTION</u> | <u>TITLE</u> |
|----------------|--|
| 1. | Legal Responsibility |
| 2. | Assessment of CCTV Appropriateness 1. Fixed Installation CCTV Systems |
| 3. | Assessment of CCTV Appropriateness 2. Fire Appliance CCTV Systems |
| 4. | Purpose of the Scheme |
| 5. | 1. Fixed Installation CCTV Policy 1.1 The Siting Of Fixed Installation CCTV 1.2 Image Quality 1.3 Recording Procedure 1.4 Training 1.5 Maintenance Policy |
| 6. | 2. Fire Appliance CCTV Policy 2.1 The Siting Of Vehicle Mounted CCTV 2.2 Image Quality 2.3 Recording Procedure 2.4 Training 2.5 Maintenance Policy |
| 7. | Recorded Image Security |
| 8. | Access and Disclosure Of Recorded Images To Third Parties |
| 9. | Access by Data Subjects |
| 10. | Access and Disclosure of Images for Training Purposes, Equipment Evaluation and Media Purposes |
| 11. | Requests to Prevent the Processing Of Data |
| 12. | Comments, Complaints and Appeals Procedure |
| 13. | Responsible Person for and Monitoring of Code Of Practice Compliance |

Appendix A SYFRA Premises Operating CCTV

Appendix B Vandalism Costs Accrued at BTC

Appendix C Attacks on Firefighters



Legal Responsibility

South Yorkshire Fire and Rescue Authority (SYFRA) own and operate Closed Circuit Television (CCTV). Legal responsibility resides with South Yorkshire Fire and Rescue (SYFR).

For the purpose of this document SYFR and SYFRA are inseparable bodies and the term 'Authority' refers to both parties unless otherwise made clear.



Assessment of CCTV Appropriateness

1. Fixed Installation CCTV

SYFRA own and operate fixed installed CCTV systems at a number of its Premises (Appendix A) for the following purposes:-

- To reduce crime in the form of theft, fire, vandalism, physical and verbal abuse to its personnel and property providing prevention through deterrent and detection. Recorded images may be used as evidence against the perpetrators of unlawful activity;
- To provide a safer and a more secure environment for all personnel working within the premises or any members of the public with lawful reasons for being at the premises;
- Maintain the security of its buildings and associated contents;
- Monitoring of training, performance and quality.

Under Health and Safety Legislation SYFRA are fully committed to the duty of care for its employees, and all other persons using or visiting its premises.

The hierarchy of control measures to eliminate and reduce risk engaged by SYFRA cannot guarantee against criminal activity being undertaken against its personnel or its property.

Over recent years the number of acts of vandalism and criminal activity performed against fire service property, its personnel and their property has risen alarmingly with little or no action being taken against the perpetrators. The damage caused to property amounts to many thousands of pounds (Appendix B). This public funding could more appropriately be spent on critical areas to improve working environments and make communities safer.

SYFRA regards Fixed Installation CCTV systems as an important tool to deter criminal attacks on personnel and property and where they do occur, aid the prosecution of perpetrators, making working environments and communities safer.

SYFRA does not regard CCTV systems to be the solution to criminal activity, but one of numerous tools deployed to reduce the number of criminal incidents on its property and personnel.

2. Fire Appliances CCTV Systems

SYFRA have deployed Mobile CCTV systems mounted on all Fire appliances to assist in establishing safer working environments for Fire and Rescue Service Personnel and the communities they serve.

This assessment provides justification for the use of CCTV for the purpose of reducing crime in the form of assaults/attacks on firefighters by aiding prevention through deterrence, and detection. Recordings of any attacks may be used as evidence against the perpetrators of such attacks. It is also the intention to use this system for fire investigation, accident investigation, equipment evaluation, and to create a knowledge pool to offer good learning experiences for improvements in operational tactics and command, promote community safety and education utilising the media and monitoring of training, performance and quality.

Under Health and Safety legislation SYFRA has a duty of care for its employees.

The hierarchy of control measures to eliminate and reduce risk, employed by SYFRA cannot completely protect against the indiscriminate attacks experienced by firefighters.

It is evidenced in Appendix C that the number of attacks that firefighters have to endure is too high, that the number of attacks is increasing, that all firefighters respond to 'at risk' Station areas and that the most likely form of attack is by projectile.

Not recorded within this assessment, but documented within national returns (Fires of Special Interest Category C - Attacks on Fire Service Personnel) (FOSI Category C) to Her Majesty's Fire Service Inspectorate (HMFSI) is evidence that these 'attacks' occur during the morning, afternoon, evening and night time. Based upon this evidence SYFRA will operate CCTV on all occasions that fire appliances are in use.

SYFRA regard CCTV systems mounted on fire appliances as an important tool to deter attacks on firefighters and where they do occur, aid prosecution of perpetrators, making working environments and communities safer.

SYFRA does not regard CCTV as the total solution but one of many tools employed to reduce the incidents of attack.

Purpose of Scheme

SYFRA own and operate CCTV systems for the purpose of:-

a) Fixed installation CCTV systems

- To reduce crime in the form of theft, fire, vandalism, physical and verbal abuse to its personnel and property by aiding prevention through deterrence and detection. Recorded activity may be used as evidence against the perpetrators of unlawful activity;
- To provide a safer and a more secure environment for all personnel working within the premises, or any members of the public with lawful reasons for being at the premises;
- Maintain the security of its buildings and associated contents;
- Monitoring of training, performance and quality.

b) Mobile CCTV systems mounted on fire appliances for the purpose of:-

- To reduce crime in the form of assaults/attacks on firefighters by aiding prevention through deterrence, and detection. Recordings of any attacks/assaults may be used as evidence against the perpetrators of such attacks;
- To reduce crime in the functions outlined under the 2004 Fire and Rescue Services Act by aiding prevention through deterrence, and detection. Recordings of any incidents may be used as evidence against perpetrators;
- Fire Investigation;
- Accident Investigation;
- Equipment evaluation;
- Provision of a knowledge pool to offer good learning experiences, and improvements in operational tactics and command;
- Promote community safety and education utilising the Media;
- Monitoring of training, performance and quality.

1. Policy – Fixed Installation CCTV

The following statutory requirements must be observed and complied with when utilising fixed CCTV systems:-

- Data Protection Act 1998;
- Regulation of Investigatory Powers Act 2000;
- European Convention on Human Rights;
- Freedom of Information Act 2000.

The fixed installed close circuit television (CCTV) system will only be used within the Data Protection Act 1998 Code of Practice, Regulation of Investigatory Powers Act 2000 and the European Convention of Human Rights to provide a safe working environment for SYFR personnel and any member of the public with lawful reason for being within the grounds or premises of Fire Service property.

To assist compliance with the Data Protection Act, the following principles must be adhered to:-

- Fixed Installed CCTV must have a documented purpose for intended use;
- Operating procedures must be established and documented;
- Disclosure policies must be established and documented;
- Operators of the camera equipment must be competent and trained in the use of such camera equipment;
- All premises must have clear signage indicating CCTV in use and a telephone point of contact included.

This Policy provides for compliance with these principles.

The use of fixed installed CCTV systems does not generally fall within the provisions of the Regulation of Investigatory Powers Act 2000, which only applies to 'Covert or Directed' Surveillance. The fixed installed CCTV system will not be used for anticipated targeted surveillance. To comply with the Regulation of Investigatory Powers Act any requirement to undertake anticipated targeted surveillance will be performed under Policy 3 - Covert Surveillance or by South Yorkshire Police.

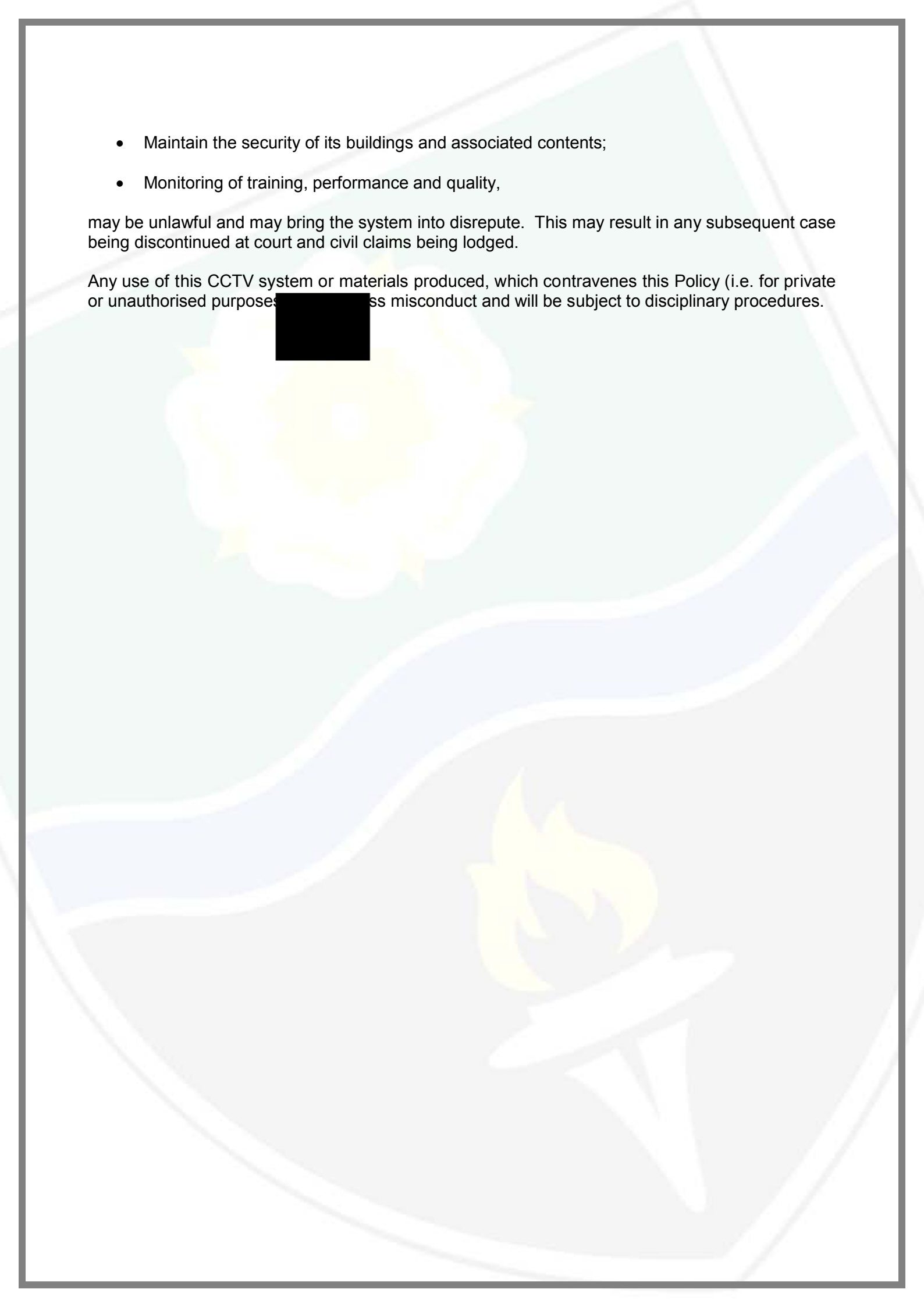
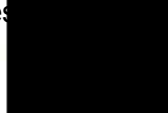
The use of CCTV for purposes other than:-

- To reduce crime in the form of theft, fire, vandalism, physical and verbal abuse to its personnel and property by aiding prevention through deterrence and detection. Recorded images may be used as evidence against the perpetrators of unlawful activity;
- To provide a safer and a more secure environment for all personnel, whether working within the premises or any members of the public with lawful reasons for being at the premises;

- Maintain the security of its buildings and associated contents;
- Monitoring of training, performance and quality,

may be unlawful and may bring the system into disrepute. This may result in any subsequent case being discontinued at court and civil claims being lodged.

Any use of this CCTV system or materials produced, which contravenes this Policy (i.e. for private or unauthorised purposes) is misconduct and will be subject to disciplinary procedures.



1.1 The Siting of Fixed Installed CCTV System

The Fixed CCTV surveillance system will continuously record from all cameras 24 hours per day. The fixed cameras will record a set surveillance area whereas the omni-directional cameras will record a set surveillance area but will react to movement where specific movement is detected.

The cameras have been positioned so that no visible access can be made to domestic dwellings, toilets, bathrooms and areas of personnel privacy including prayer rooms.

In siting and maintaining [REDACTED] equipment the Authority will ensure that:-

- The location of cameras is justified by the stated purpose as outlined in the Fixed Installation CCTV Policy
- The equipment should as far as practicable and possible, continually operate effectively and efficiently
- The image quality is maintained on the reproduction to disk
- There are records of use, including duration and reasons for downtime, maintenance and repair of equipment, including the time elapsed between failures and repairs. Periodic review of records, by the Data Protection Officer or his/her assignee, should be recorded.

Operators will receive training and demonstrate competence in:-

- The purpose of the system;
- Equipment use to achieve system purpose;
- Recognition of the privacy implications of the area covered.

All SYFR buildings/premises fitted with CCTV systems will prominently display public awareness signs detailing:-

- CCTV equipment in operation;
- Purpose of the CCTV system;
- Contact telephone number.

1.2 Image Quality

The Fixed CCTV cameras record images onto a computer hard drive operating on a six day loop (i.e. when the recording hard drive is full it automatically records over the previous images). Access to this hard drive will be restricted to a trained team, nominated and under the direct control of the Data Protection Officer.

The equipment will be checked DAILY to ensure performance quality and that the system is fully operational. Appropriate checks will be taken on identification of unsatisfactory performance and will be documented in accordance with equipment maintenance procedures.

The system overwrite function for date/time, frame reference and camera location will be checked and documented for accuracy.

1.3 Recording Procedures

The equipment will record data from all Fixed Installed cameras 24 hours per day onto a computer hard drive. The captured data will automatically be recorded onto a hard drive within a locked cabinet and will be stored on the hard drive for six days. After the sixth day the data will be overwritten by newly captured data.

Access to recorded images on the hard drive will only be made after the appropriate authorisation is given.

Access to recorded images on the hard drive is restricted to the trained team nominated and under the direct control of the Data Protection Officer.

1.4 School Training

Operators

Appropriate training will be provided in accordance with the CCTV code of practice.

ICT will arrange for introductory and familiarisation training, in the use of the system, to all personnel required to operate the CCTV system.

The systems may vary between sites and personnel will be nominated for training.

At the Brigade Training Centre the Centre Manager will nominate staff to operate the system. Those nominated are the Centre Manager, Caretaker and Audio Visual Technician.

Operators will receive training and will be required to demonstrate competence in:-

- The purpose of the system;
- Rights of individuals under the CCTV system;
- SYFRA Disclosure Policy;
- Equipment used to achieve scheme purpose;
- Recognition of the privacy implications of the area covered;
- Recognition that images may only be viewed by authorised employees of SYFRA.

Only operators who have received training and are deemed competent can operate the system.

Equipment operation will be provided initially by the installation/security company who have fitted the cameras / computer based Fixed Installed CCTV system.

Support Staff

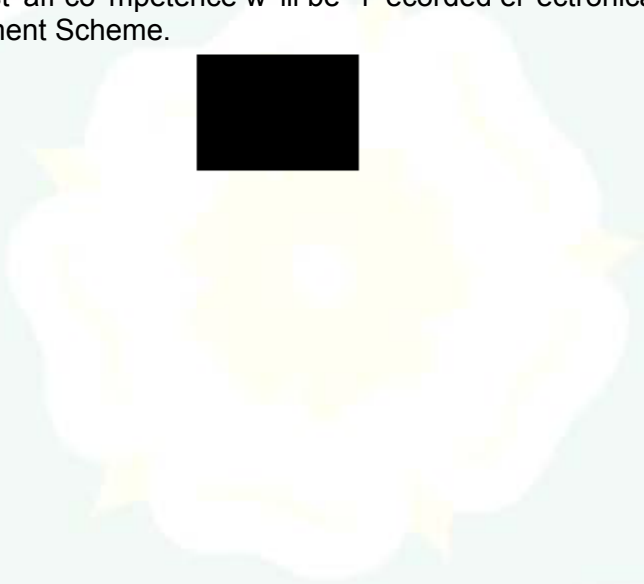
ICT will arrange for introductory and familiarisation training for the nominated team as specified by the Data Protection Officer:-

- a) The purpose of the scheme;
- b) Rights of individuals under the scheme;
- c) Equipment use to achieve scheme purpose;
- d) Recognition of the privacy implications of the space covered;
- e) Recognition that images may only be viewed by authorised employees of SYFRA;
- d) Image down load, evidential continuity, image security procedures;
- e) Disclosure Procedures;
- f) Access Procedures;

g) Viewing Procedures;

h) Procedures for identifying requests to prevent processing likely to cause substantial and unwarranted damage to individuals and prevent automated decision taking in relation to that individual.

Support staff competence will be recorded electronically and reviewed through the Staff Development Scheme.



1.5 Maintenance Policy

The overall maintenance of the system will be the responsibility of the Estates Department. A maintenance contract will be adhered to by the CCTV system installation contractor who will respond to all defects of the CCTV computer system and any cameras associated with the installation.

The Brigade electrical engineers will maintain CCTV cameras that were not part of the initial installation.

The operators will check [REDACTED] on a daily basis to ensure performance and reliability. The Buildings Manager will be informed of any malfunction/unsatisfactory performance and he/she will inform the Estates Section in accordance with equipment maintenance procedures.

Only competent qualified engineers will be authorised to carry out maintenance on the fixed installed CCTV system.

The system overwrite function for date/time, frame reference and camera locations shall be checked and documented for accuracy.

All servicing and maintenance on the system must be recorded/documentated in the maintenance log.

2 Policy – Fire Appliance CCTV

The following statutory requirements must be observed and complied with when utilising mobile CCTV:

Data Protection Act 1998;

Regulation of Investigatory Powers Act 2000;

European Convention on Human Rights;

Freedom of Information Act 2000.

The vehicle mounted closed circuit television (CCTV) system will only be used within the Data Protection Act 1998 Code of Practice, Regulation of Investigatory Powers Act 2000 and the European Convention of Human Rights to provide a safe working environment for SYFRS personnel and any member of the public with lawful reason for being at that location when SYFRS are operating in the community.

To assist compliance with the Data Protection Act, the following principles must be adhered to:

Mobile CCTV must have a documented purpose for intended use;

Operating procedures must be established and documented;

Disclosure policies must be established and documented;

Operators of the camera equipment must be competent and trained in the use of such camera equipment;

Each Appliance/vehicle must be clearly marked, indicating CCTV in use and a telephone point of contact included.

This Policy provides for compliance with these principles.

The use of fire appliance mounted CCTV does not generally fall within the provisions of the Regulation of Investigatory Powers Act 2000, which only applies to “Covert or Directed” surveillance. The fire appliance mounted CCTV system will not be used for anticipated targeted surveillance.

The use of CCTV for purposes other than:

- To reduce crime in the form of assaults/attacks on firefighters by aiding prevention through deterrence, and detection. Recordings of any attacks/assaults may be used as evidence against the perpetrators of such attacks;
- To reduce crime in the functions outlined under the Fire and Rescue Services Act 2004 by aiding prevention through deterrence, and detection. Recordings of any incidents may be used as evidence against perpetrators;
- Fire Investigation;
- Accident Investigation;

- Equipment evaluation;
- Provision of a training knowledge pool to offer good learning experiences and improvements in operational tactics and command;
- Promote community safety and education utilising the Media;
- Monitoring of training, performance and quality,

may be unlawful and may damage the system into disrepute. This may result in any subsequent case being discontinued at court or claims being lodged.

Any use of this CCTV system or materials produced, which contravenes this Policy (i.e. for private or unauthorised purposes) will be gross misconduct and will be subject to disciplinary procedures.

2.1 The Siting of Vehicle Mounted CCTV System

The Vehicle Mounted CCTV surveillance is activated by the vehicle ignition switch and covers the working environment (360°) surrounding a Fire Appliance.

In siting and maintaining the CCTV equipment the authority will ensure that:-

- a) The location of cameras is justified by the stated purpose as outlined in the CCTV scheme;
- b) The equipment shall, as practicable and possible, continually operate effectively and efficiently;
- c) The image quality is maintained on the reproduction to disk;
- d) There are records of use, including duration and reasons for downtime, maintenance and repair of equipment, including the time elapsed between failures and repairs. Periodic review of records, by the ICT Manager or their assignee, should be recorded.

Operators will receive training and demonstrate competence in:-

- a) The purpose of the scheme;
- b) Equipment use to achieve scheme purpose;
- c) Recognition of the privacy implications of the space covered.

All vehicles will prominently display public awareness signs detailing:-

- a) CCTV equipment in operation;
- b) Scheme purpose;
- d) Contact details.

2.2 Image Quality

The cameras (of which the in-cab camera can be tilted panned and zoomed to enhance images) will record images on a computer hard drive operating on a 64hour loop (i.e. when the recording equipment is full it automatically records over the previous images). Access to this hard drive will be restricted to a trained team, nominated and under the direct control of the Data Protection Officer.

The equipment shall be [REDACTED] ensure performance quality on installation and as determined by CCTV Contractor. [REDACTED] action will be taken on identification of unsatisfactory performance and will be [REDACTED] in accordance with equipment maintenance procedure.

The system overwrite function for date/time, frame reference shall be checked and documented for accuracy.

2.3 Recording Procedures

The equipment used records automatically on the activation of the vehicle ignition key. The equipment adds the location, date, time, vehicle speed, blue lights and sirens, braking and indicators.

Fire crews can not interact or influence the recording of images utilising the fixed cameras.

If occurrences exist which fall within the purpose of the CCTV scheme the moveable fixed camera shall be manipulated manually (pan, tilt, rotation and zoom) to capture appropriate enhanced quality images of the incident. [REDACTED]

If occurrences exist which fall within the purpose of the CCTV scheme the system microphone can be activated by the appliance Crew/Watch Commander. The decision when to commence recording sound is that of the Appliance Crew/Watch Commander. Private conversations between members of the public shall not be recorded.

2.4 Training

Operators

Appropriate training will be provided in accordance with the CCTV code of practice.

Training staff will arrange for introductory and familiarisation training, in the use of the system, to each Station required to operate the CCTV system.

Operators will receive training to demonstrate competence in:-

- a) The purpose of the scheme;
- b) Rights of individuals under the scheme;
- c) SYFRA Disclosure Policy;
- d) Equipment use to achieve scheme purpose;
- e) Recognition of the privacy implications of the space covered;
- f) Recognition that images may only be viewed by authorised employees of SYFRA.

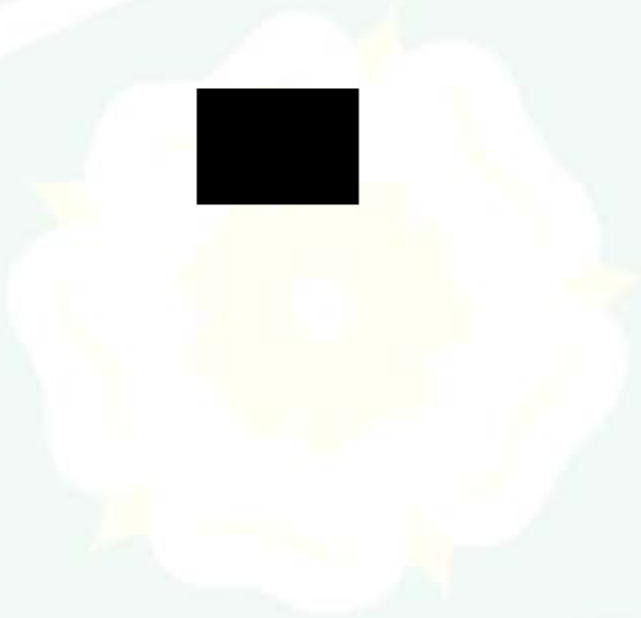
Only operators who have received training are deemed competent and should be the only people to operate the system. Operator competence will be recorded on the 'Redkite'.

Support Staff

ICT will arrange for introductory and familiarisation training for the nominated team as specified by the ICT Manager:-

- a) The purpose of the scheme;
- b) Rights of individuals under the scheme;
- c) Equipment use to achieve scheme purpose;
- d) Recognition of the privacy implications of the space covered;
- e) Recognition that images may only be viewed by authorised employees of SYFRA;
- f) Image download, evidential continuity, image security procedures;
- g) Disclosure Procedures;
- h) Access Procedures;
- i) Viewing Procedures;
- j) Procedures for identifying requests to prevent processing likely to cause substantial and unwarranted damage to individuals and prevent automated decision taking in relation to that individual.

Support staff competence will be recorded electronically and reviewed annually.



2.5 Maintenance Policy

A maintenance log will be kept for each CCTV unit. All performance quality checks, defects and corrective action is to be recorded and authenticated within this log.

The equipment shall be checked to ensure performance quality on installation and as outlined by 'Contractors Preventative Maintenance Schedule'.

The following performance [REDACTED] checked by the Contractor to ensure correct functionality:-

- a) Image quality; [REDACTED]
- b) System overwrite function for date/time;
- c) System overwrite, vehicle speed, blue lights, siren, braking and indicators;
- d) Monitor functionality;
- e) Camera control;
- f) Download capability;
- g) Downloaded image quality.

Unsatisfactory performance shall be recorded in the Maintenance Log (which will automatically update the central data base) and shall be reported immediately to the ICT Manager by telephone.

The ICT Manager will:-

- a) Determine if the defect can be rectified by South Yorkshire Fire and Rescue personnel. If this is possible make appropriate arrangements to restore the system to full functionality. This shall be as soon as practicable, but shall be within 24 hours;
- b) When the defect cannot be rectified by South Yorkshire Fire and Rescue personnel, arrange for the contractor to take appropriate action. The System shall be restored to full functionality as soon as practicable, but this shall be within 1 working day (next full working day at the weekend).

The repair shall be recorded and authenticated within the maintenance log.

The ICT Manager shall monitor the quality of the maintenance work.

When the fire appliance is not being used for its intended purpose (e.g. at workshops for servicing), the date, time, reason shall be recorded in the maintenance log by the Officer in charge of the fire appliance (O.I.C.).

When the fire appliance is returned to normal use, the date and time shall be recorded in the maintenance log by the Officer in charge of the fire appliance (O.I.C.).

Recorded Image Security

Access to recorded images on the hard drive will only be made after the appropriate authorisation is given.

Access to recorded images on the hard drive is restricted to the trained team nominated and under the direct control of the Data Protection Officer.

All access to the recorded  shall be recorded in the **CCTV Data Base application**.

All recorded images accessed and downloaded on to disc will be given a unique reference number. This number will be the number of the disc generated on a given date e.g. 3 – 17/09/06.

The viewing of images recorded by all CCTV will only take place in a restricted area. No unauthorised person will have access to this location while viewing is taking place.

Downloaded images shall be stored in a locked safe. Removal of the media on which images are recorded from the locked safe, for viewing purposes, shall be recorded in the CCTV Data Base application and is documented as follows:-

- a) The date and time of removal;
- b) The name of the person removing the images;
- c) The name(s) of the person(s) viewing the images. If this should include third parties, include the organisation of that third party;
- d) The reason for the viewing;
- e) The outcome, if any, of the viewing;
- f) The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.

THE ONLY COPIES OF RECORDED IMAGES TO BE MADE ARE THOSE OUTLINED IN THIS POLICY. ALL OTHER COPYING OF RECORDED IMAGES IS STRICTLY PROHIBITED.

Images of Evidential Value - Unedited

On authorisation, for the disclosure of recorded images, the access to the hard drive will be recorded in the **CCTV Data Base application**, as shall the following information:-

- a) The date on which the images were removed from the general system for use in legal proceedings;
- b) The reason why they were removed from the system;
- c) Any crime incident number to which the images may be relevant;
- d) The location of the images;
- e) Signature of collecting Police Officer where appropriate.

Two identical discs will be generated and shall be:-

- a) Uniquely numbered;
- b) Sealed with specified label/bag;
- c) Recorded in the continuity log.

One disc shall be retained by SYFRA and kept in a locked safe, Information and Communication Technology Section (ICT) and Headquarters (CHQ). All access to this disc shall be recorded in the **CCTV Data Base application**.

The second disc shall be given to (recorded in the **CCTV Data Base application**), viewed by (Recorded in the **CCTV Data Base application**) third party.

Images of Evidential Value - edited

Access to recorded images on the hard drive will only be made after the appropriate authorisation is given.

Access to recorded images on the hard drive is restricted to the trained team nominated and under the direct control of the Data Protection Officer.

All access to the recorded images shall be recorded in the **CCTV Data Base application** as shall the following information:-

- a) The date on which the images were removed from the general system for use in legal proceedings;
- b) The reason why they were removed from the system;
- c) Any crime incident number to which the images may be relevant;
- d) The location of the images.

Three discs shall be generated and shall be:-

- a) Uniquely numbered;
- b) Sealed with specified label/bag;
- c) Recorded in the continuity log.

One disc, unedited, shall be retained by SYFRA and kept in a locked safe, ICT, CHQ. All access to this disc shall be recorded in the **CCTV Data Base application**.

The second disc shall be edited by ICT in accordance with legal advice, to mask the identity of specified individual(s). It shall be retained by SYFRA, being kept in locked safe, ICT Dept, CHQ, with the first disc. All access to this disc shall be recorded in the **CCTV Data Base application**.

The Third disc shall be identical to the second disc. It shall be given to, or viewed by the third party (Recorded in the **CCTV Data Base application**).

Images for Data Subjects, Media, Training, Performance and Quality Purposes, and Equipment Evaluation

Access to recorded images on the hard drive will only be made after the appropriate authorisation is given.

Access to recorded images on the hard drive is restricted to the trained team nominated and under the direct control of the Data Protection Officer.

All access to the recorded [REDACTED] shall be recorded in the **CCTV Data Base application**.

- a) The date on which the images were removed from the general system;
- b) The reason why they were removed from the system;
- c) Any crime incident number to which the images may be relevant;
- d) The location of the images

Three discs shall be generated and shall be:-

- a) Uniquely numbered;
- b) Recorded in the continuity log.

One disc, unedited, shall be retained by SYFRA and kept in a Locked Safe, ICT, CHQ. All access to this disc shall be recorded in the **CCTV Data Base application**.

The second disc shall be edited by ICT, in accordance with legal advice where required, to mask the identity of specified individual(s). It shall be retained by SYFRA, being kept in a Locked safe, ICT, CHQ with the first disc. All access to this disc shall be recorded in the **CCTV Data Base application**.

The Third disc shall be identical to the second disc. It shall be given to (recorded in the **CCTV Data Base application**), viewed by (Recorded in the **CCTV Data Base application**) third party.

A log shall be held in ICT of all discs produced for training and equipment evaluation purposes. The log shall also record the location of each disc.

Unavailability of Editing Facilities

When editing facilities are not available in-house, an editing Company may be hired to carry it out.

When/if an editing Company is hired or the media Organisation receiving the images undertakes to carry out the editing, then the Data Protection Officer or designated member of staff needs to ensure that:-

1. There is a contractual relationship between the data controller and the editing Company;
2. That the editing Company has given appropriate guarantees regarding the security measures they take in relation to the images;
3. The manager has checked to ensure that those guarantees are met;

4. The written contract makes it explicit that the editing Company can only use the images in accordance with the instructions of the manager or designated member of staff;
5. The written contract makes the security guarantees provided by the editing Company explicit.

It is accepted that, in these circumstances, failure on the part of the media representative (the agent) to adequately mask the identity of an individual, or individuals, may result in action being taken against the authority (the principal) not the media representative.

Retention of Recorded Images

All evidence will be retained in accordance with the Data protection Act 1998 and the Freedom of Information Act 2000.

SYFRA will keep recorded images for the minimum period required, to enable the images to fulfil the function for which they were downloaded (or as long ordered by the Courts), after which they will be destroyed.

The destruction of all discs shall be entered in the **CCTV Data Base application**.

Access to and Disclosure of Recorded Images to Third Parties

Disclosure of the recorded images to third parties will only be made in the following limited and prescribed circumstances:-

Unedited discs:-

- Law Enforcement and National Security Agencies to assist in a specific criminal enquiry;
- Prosecution Agencies.

b) Edited discs, where, when appropriate the identity of certain or all individuals is masked:-

- Relevant legal representatives;
- The media where it is decided public assistance is required to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. The wishes of the victim(s) in the incident will be taken into account;
- Media Agencies;
- People whose images have been recorded and retained (unless disclosure would prejudice criminal enquiries or criminal proceedings).

Disclosure Requests

Any requests for disclosure must be written and delivered to the Data Protection Officer within 60 hours (it may be possible to action requests after 60 hours, however as the images may have been overwritten after this duration, this can not be guaranteed), clearly stating the reasons for this request.

The Data Protection Officer will request, authorisation for disclosure, from the Disclosure Officer (or their nominated officer).

The Disclosure Officer (or their nominated officer) will consult legal services if required.

In the event of the Data Protection Officer being unavailable then the Disclosure Officer (or their nominated officer) must be contacted.

In the event that the Disclosure Officer (or their nominated officer) is unavailable the Duty Principal Officer shall be contacted for authorisation.

Requests from the Police, Law Enforcement or National Security Agencies must be referred to the Disclosure Officer (or their nominated officer). Where requests are made out of 'Normal' working hours and are required immediately, Fire Control will manage disclosure by contacting the 'Duty Principal Officer', who will have overall responsibility for disclosure. On receiving disclosure authorisation, the Data Protection Officer will arrange the data transfer to disc according to continuity of evidence requirements.

Recording of Disclosure Requests

All requests for access or disclosure shall be recorded in accordance with the Freedom of Information Act 2000 and the Data Protection Act 1998.

Guidance on Disclosure

In the event of a recording of evidential value and a working copy or stills are required, these will be compiled in accordance with the following guidance and instruction from the Disclosure Officer (or their nominated officer), where required, following consultation with Legal Services.

Printed images taken from recordings as a still or snapshot are subject to the same controls and principles of Data Protection, as any other information held.

Access by Data Subject

Requests for information by Data Subjects will be actioned inline with the Data Protection Act. Since the system will be indiscriminate in the recording of data it will be necessary to edit images in order to respond to requests for access to personal data.

Contact Point

The contact point indicated on the RA CCTV signs is available to members of the public during office hours.

Individuals requesting access to recorded images will be provided on request with one or more of the following:

- a) The leaflet which individuals receive when they make a subject access request as general information;
- b) A copy of the CCTV Code of Practice;
- c) A subject access request form if required or requested;
- d) The complaints procedure to be followed if they have concerns about the use of the system;
- e) The complaints procedure to be followed if they have concerns about non-compliance with the provisions of this Code of Practice.

Access/Disclosure Requests

Contact details for 'Data Subject' access requests are available at:

South Yorkshire Fire and Rescue Service
Command Headquarters
Wellington Street
Sheffield
S1 3FG

Telephone 0114 2532599

Data subjects will complete a standard Data Subject Access Request form which:

- a) Defines the Data Subjects rights under the Data Protection Act 1998;
- b) Requires the provision of sufficient information for the Data Protection Manager to establish the true identity of the applicant;
- c) Requires the provision of sufficient information for the Data Protection Manager to identify and locate the images requested, including dates, times and locations;
- d) Indicates that the response will be prompt and in any event will be within 40 days;

e) Requires the applicant to choose whether to simply view the disc or to receive a copy.

The Data Protection Officer will request, authorisation for access/disclosure, from the Disclosure Officer (or their nominated officer).

The Disclosure Officer (or their nominated officer) will consult legal services if required.

In the event of the Data Protection Officer being unavailable then the Disclosure Officer (or their nominated officer) must be contacted.

In the event the Disclosure Officer (or their nominated officer) is unavailable the Duty Principal Officer shall be contacted.

On receiving access/disclosure authorisation, the Data Protection Officer will arrange the data transfer to disc according to continuity of evidence requirements.

The Data Protection Officer will monitor the retrieval and the access/disclosure of the Personal Data to the Data Subject, to ensure that images of third parties are not disclosed. If third party images are not to be disclosed, the ICT Manager shall arrange for third party images to be disguised or blurred.

Recording of Access/Disclosure Requests

All requests for access or disclosure shall be recorded in accordance with the Freedom of Information Act 2000 and the Data Protection Act 1998.

Access to and Disclosure of Images for Media, Training, Performance and Quality Purposes, and Equipment Evaluation

Images recorded by the system may be used for media, training, performance and quality, and equipment evaluation purposes. Since the system will be indiscriminate in the recording of data it may be necessary to edit images in order to respond to requests for access to this data.

Internal requests for disclosure of images will be considered and documented with the same robustness as external requests.

Access/Disclosure Requests

To ensure the availability of images any requests for disclosure must be written and delivered to the Data Protection Officer within 60 hours, clearly stating the reasons for this request. After that period images may be available but can not be guaranteed as this is dependant on fire appliance activity.

The Data Protection Officer will request authorisation for disclosure from the Line Manager of the person making the request who shall be the minimum role of District Manager.

The Line Manager/District Manger will consult Legal Services if required.

In the event of the Data Protection Officer being unavailable then the Disclosure Officer (or their nominated officer) must be contacted.

In the event that the Line manager / Disclosure Officer (or their nominated officer) is unavailable the next tier of line management/Duty Principal Officer shall be contacted.

No disclosure shall be made until the images are viewed by the disclosing District Manager/Line Manager to ensure South Yorkshire Fire and Rescue Authority is not compromised by the disclosure.

Recording of Access/Disclosure Requests

All requests for access or disclosure shall be recorded in accordance with the Freedom of Information Act 2000 and the Data Protection Act 1998.

Request to Prevent the Processing of Data

All requests from individuals to:

- a) Prevent processing likely to cause substantial and unwarranted damage to that individual,
- b) Prevent automated decision taking in relation to that individual,

must be passed to the Data Protection Officer who will make the decision whether the request will be complied with or not.

The Data Protection Officer will provide a written response to the individual within 21 days of receiving the request setting out their decision on the request.

When the decision is made that the request will not be complied with, the reasons must be detailed in the response to the individual.

A copy of the request and response will be retained.

The Data Protection Officer shall document:

- a) The decision;
- b) The request from the individual;
- c) Their response to the request from the individual.

Comments, Complaints and Appeals

SYFRS is committed to providing a quality service 24 hours a day, every day, to meet the requirements of the people of South Yorkshire, visitors, or people passing through the County. If an applicant is unhappy with the response of SYFRS and wishes to make a complaint about the way their application for information has been dealt with they may do so verbally, or in writing, or by e-mail, addressing their complaint to:-

The Data Protection Officer
South Yorkshire Fire and Rescue Service
Command Headquarters
Wellington Street
Sheffield
S1 3FG

Telephone 0114 2532251

Fax 0114 2532398

E-mail servicedesk@syfire.gov.uk

A log will be maintained to record the number and nature of complaints or enquiries received together with an outline of the action taken.

Should the applicant remain dissatisfied with the way that the SYFRA has dealt with the application the Officers of the Service will give every possible assistance in the preparation of an appeal to the Information Commissioner.

The Commission has set up a public inquiry service which may be contacted:-

by telephone on:- (01625) 545745

or by E-mail at: data@dataprotection.gov.uk

or by post to:-
The Information Commission
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

An annual report detailing numbers and nature of complaints will be published by the Data Protection Officer in order to assess public reaction to and opinion of the use of the system.

Responsible Persons for and Monitoring of Code of Practice Compliance

The Data Controller (SYFRA) is responsible for CCTV Policy and Procedures including, disclosure and disclosure Policies. Within the Authority the nominated responsible person is the ACO Community Safety (Disclosure Officer) or their nominated officer.

The ICT Manager is responsible for recorded image management and security.

The ICT Manager is responsible for document management and security.

The ICT Manager is responsible for the day to day operation and maintenance of the CCTV equipment.

Each employee is individually responsible, and is required to work to this Policy in accordance with the principles specified in the Data Protection Act 1998.

The ICT Manager will annually:

- a) Review documented procedures to ensure that the provisions of this Code are being complied with;
- b) Compare **CCTV Data Base application** with the hard drives access record to ensure no unauthorised access has taken place;
- c) Sample recorded images to ensure the equipment is being used for its intended use only;
- d) Monitor the quality of the maintenance work.

A report on this review shall be provided to the data controller (SYFRA) in order that compliance with legal obligations and provisions with this Code of Practice can be monitored.

An internal annual assessment will be undertaken by the ICT Manager to evaluate the effectiveness of the system.

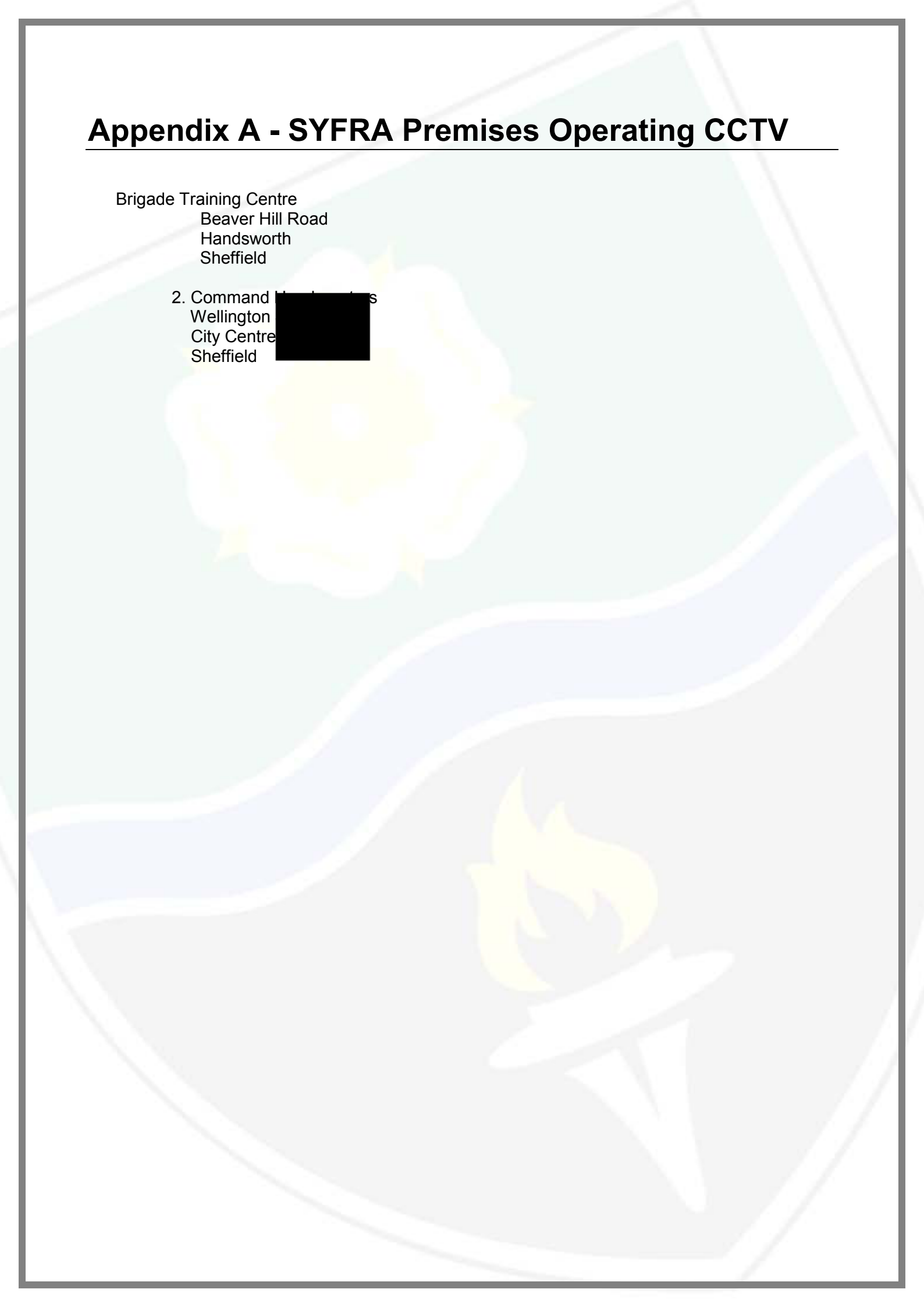
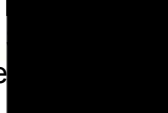
The results of the report will be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it will be discontinued or modified.

The result of these reports will be made publicly available.

Appendix A - SYFRA Premises Operating CCTV

Brigade Training Centre
Beaver Hill Road
Handsworth
Sheffield

2. Command Premises
Wellington
City Centre
Sheffield



Appendix B – Vandalism Costs Accrued at BTC

Vandalism costs accrued at BTC until March 2007

The list of EST numbers is as follows:

| | | | |
|---|--|---------------------------|-----------------|
| · | 3271 & 3338 | £93.52 + £601.69 | £695.21 |
| · | 3272 | £155.44 | £155.44 |
| · | 3535 | N/A | |
| · | 3574 | £51.82 | £51.82 |
| · | 4065 | £148.01 | £148.01 |
| · | 5068 | £10.75 | £10.75 |
| · | 5346 | £461.78 | £461.78 |
| · | 5351 | £342.48 | £342.48 |
| · | 5358 | £129.52 | £129.52 |
| · | 5502 | MOD Undertook this work | |
| · | 5635 | £72.06 + £44.10 + £123.86 | £240.02 |
| · | 5658 | £58.75 | £58.75 |
| · | 5976 | | |
| | Repairs to Break in 4 December 06 | | £499.65 |
| | Roller Shutters & Boarding up of doors | | £1929.51 |
| | Total | | £4722.94 |

| | |
|--|-----------------|
| Total Cost of Vehicle Damage | £1004.56 |
| Total cost of Replacement Items | £1000.00 |
| Total Cost of Estates Repairs | £4722.94 |
| Total cost to SYF&RS BTC | £6727.50 |

Appendix C – Attacks on Firefighters

Local and national concerns are being expressed concerning the rising number of attacks on Fire Service personnel. The Chief Fire Officers Association (CFOA) and Representative Bodies strongly believe that greater protection should be afforded to our firefighters given the rising numbers of attacks they have to endure.

The total reported Fires of Significant Interest Category C (Attacks on fire service Personnel) (FOSI Cat C) notifications received by Her Majesty's Fire Service Inspectorate (HMFSI) up to 15th August 2005 were 946. [REDACTED] were reported by SYFRS. This is approximately 3.5% of the total reported incidents. (Statistics are courtesy of Jim Mann, HMA Assistant Inspector of Fire Services).

There is strong evidence that the fire service nationally and locally within South Yorkshire is susceptible to patterns of under reporting. The FBU report 'Attacks on Firefighters' also expresses concerns over the under reporting of attacks on crews.

All attacks on SYFRS crews from January 2000 to 12th March 2007 are recorded by month in Fig 1.

Fig 1. Attacks on SYFRS crews from January 2000 to 12 March 2007

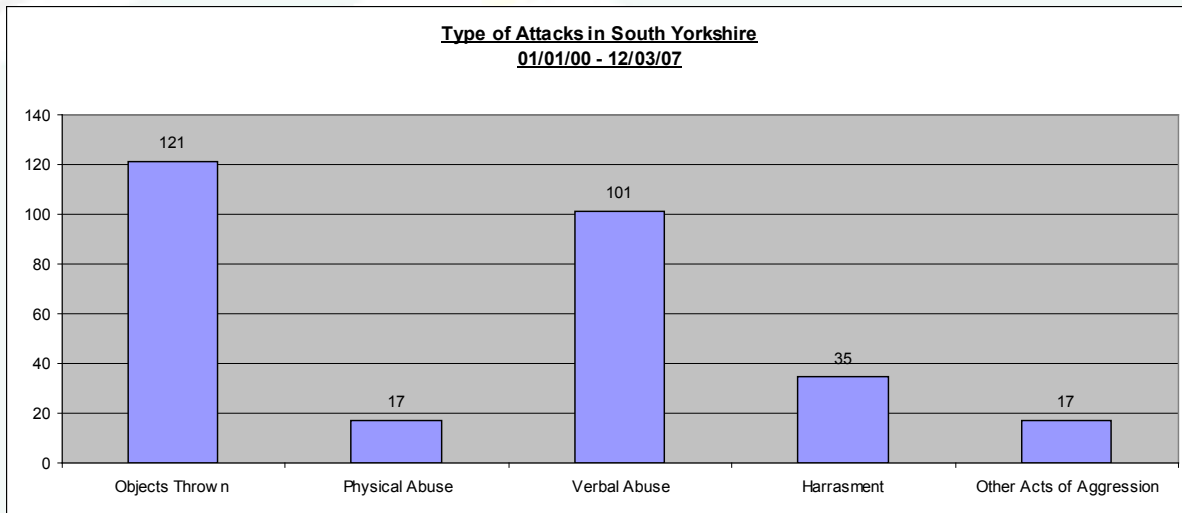
| | No. of Incidents | Objects Thrown | Physical Abuse | Verbal Abuse | Harrasment | Other Acts of Aggression | Total of Attacks |
|--------|------------------|----------------|----------------|--------------|------------|--------------------------|------------------|
| Jan-00 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Feb-00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Mar-00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Apr-00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| May-00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jun-00 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Jul-00 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Aug-00 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Sep-00 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Oct-00 | 3 | 2 | 0 | 0 | 0 | 0 | 2 |
| Nov-00 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Dec-00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jan-01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Feb-01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Mar-01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Apr-01 | 5 | 4 | 0 | 0 | 0 | 0 | 4 |
| May-01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jun-01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jul-01 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Aug-01 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Sep-01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Oct-01 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Nov-01 | 2 | 1 | 0 | 1 | 0 | 0 | 2 |
| Dec-01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jan-02 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| Feb-02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Mar-02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Apr-02 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| May-02 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Jun-02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | |
|--------------|------------|------------|-----------|------------|-----------|-----------|------------|
| Jul-02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Aug-02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Sep-02 | 3 | 3 | 0 | 0 | 0 | 0 | 3 |
| Oct-02 | 3 | 3 | 0 | 0 | 0 | 0 | 3 |
| Nov-02 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Dec-02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jan-03 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Feb-03 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Mar-03 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Apr-03 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| May-03 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Jun-03 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jul-03 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Aug-03 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| Sep-03 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Oct-03 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Nov-03 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Dec-03 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Jan-04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Feb-04 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Mar-04 | 3 | 2 | 0 | 2 | 0 | 0 | 4 |
| Apr-04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| May-04 | 2 | 2 | 1 | 1 | 0 | 0 | 4 |
| Jun-04 | 2 | 2 | 1 | 1 | 0 | 0 | 4 |
| Jul-04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Aug-04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Sep-04 | 1 | 1 | 0 | 1 | 0 | 0 | 2 |
| Oct-04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Nov-04 | 1 | 0 | 0 | 1 | 1 | 0 | 2 |
| Dec-04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jan-05 | 1 | 0 | 0 | 1 | 1 | 0 | 2 |
| Feb-05 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Mar-05 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| Apr-05 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| May-05 | 2 | 2 | 0 | 0 | 0 | 0 | 2 |
| Jun-05 | 2 | 1 | 2 | 1 | 0 | 0 | 4 |
| Jul-05 | 2 | 0 | 0 | 1 | 0 | 1 | 2 |
| Aug-05 | 6 | 4 | 1 | 4 | 2 | 0 | 11 |
| Sep-05 | 5 | 4 | 0 | 2 | 3 | 0 | 9 |
| Oct-05 | 3 | 2 | 0 | 1 | 1 | 0 | 4 |
| Nov-05 | 8 | 7 | 3 | 6 | 3 | 1 | 20 |
| Dec-05 | 5 | 3 | 3 | 5 | 3 | 2 | 16 |
| Jan-06 | 9 | 6 | 0 | 5 | 1 | 1 | 13 |
| Feb-06 | 3 | 1 | 1 | 2 | 0 | 0 | 4 |
| Mar-06 | 3 | 1 | 0 | 2 | 0 | 0 | 3 |
| Apr-06 | 10 | 5 | 1 | 7 | 2 | 0 | 15 |
| May-06 | 5 | 1 | 2 | 5 | 1 | 1 | 10 |
| Jun-06 | 7 | 3 | 0 | 3 | 2 | 0 | 8 |
| Jul-06 | 3 | 0 | 0 | 2 | 1 | 1 | 4 |
| Aug-06 | 7 | 1 | 0 | 7 | 2 | 3 | 13 |
| Sep-06 | 11 | 5 | 1 | 9 | 2 | 0 | 17 |
| Oct-06 | 13 | 11 | 0 | 7 | 3 | 2 | 23 |
| Nov-06 | 13 | 10 | 0 | 5 | 0 | 0 | 15 |
| Dec-06 | 3 | 0 | 0 | 3 | 1 | 0 | 4 |
| Jan-07 | 6 | 1 | 0 | 6 | 1 | 4 | 12 |
| Feb-07 | 9 | 4 | 0 | 6 | 4 | 1 | 15 |
| Mar-07 | 2 | 0 | 0 | 2 | 1 | 0 | 3 |
| Total | 195 | 121 | 17 | 101 | 35 | 17 | 291 |

Statistics courtesy of SYFRA Data Management Section

The maximum recorded attacks per month up to July 2005 were 5 with the occurrences of 2 or more attacks per month becoming more frequent. From August 2005 the number of reported 'attacks' has increased to an average of almost 7 per month with a maximum of 13 'attacks' reported in a 1 month period. On 15th April 2006 a firefighter suffered a serious assault which resulted in a 1 month absence from work.

Figure 2. Type of attack experienced by South Yorkshire firefighters up to 12.03.2007.



Statistics courtesy of SYFRA Data Management Section

Figure 2 is an account of the type of attack experienced by South Yorkshire firefighters up to 12 March 2007. It clearly demonstrates that the greatest risk experienced by personnel, to date, is to be struck by a projectile.

Figure 3. Number of reported 'Attacks on Crews' per Station area

Statistics courtesy of SYFRA Data Management Section

Figure 3 is an account of the number of reported 'Attacks on Crews' per Station area. Mansfield Road and Central Station areas have accounted for 31% of the total number of incidents where attacks on firefighters recorded by SYFRA have occurred. It can be seen that only 2 wholetime Station areas (Rivelin and Tankersley) and 2 Retained Station areas (Stocksbridge and Penistone) have not reported an attack. However, the fire appliances based in these Station areas routinely respond to incidents in Station areas with a history of attacks on firefighters. It is therefore

necessary to afford these firefighters with the same level of protection as those based with in the at-risk Station areas.

