West Yorkshire
Fire & Rescue Service

Closed Circuit Television (CCTV) Policy

including Silent Witness, Body Worn Video and Unmanned Aerial Vehicles

NOT PROTECTIVELY MARKED
Ownership: Corporate Services
Date Issued:18/10/2017
Version: 5.0 Status: Final

Making West Yorkshire Safer
www.westyorksfire.gov.uk

Revision and Signoff Sheet

Change Record

Date	Author	Version	Comments
20/01/2014	Allan Darby	2.1	
19/02/2014	Allan Darby	2.2	Minor amendments throughout
09/06/2014	Allan Darby	3.1	Minor changes following ICO advice
04/04/2017	Allan Darby	4.1	Amendments to stated purposes and the AIR procedure

Reviewers

Name	Version Approved	Position	Organisation	Date
Michael Barnes	3.0	Chief Legal and Governance Officer	WYFRS	19/03/2014
Anne Russell	4.0	Senior Policy Officer, Public Security Group	ICO	09/06/2014
IG Policy Consultation Group	5.0	IGSG	WYFRS	26/05/2017

Distribution

Name	Position	Organisation
All WYFRS Staff		WYFRS

Document Properties

Item	Details

Document Title	Closed Circuit Television (CCTV) Policy
Author	Administrator
Creation Date	19 March 2014
Last Updated	19 October 2017

Contents

1 Introduction

West Yorkshire Fire and Rescue Authority (WYFRA) own and operate Closed Circuit Television (CCTV) to provide a safe and secure environment for staff and visitors, and to protect Authority property. The legal responsibility for the CCTV lays with West Yorkshire Fire and Rescue Service (WYFRS).

This document sets out the accepted use and management of the CCTV equipment and images to ensure the Authority complies with the Data Protection Act 1998, Human Rights Act 1998 and other legislation. It has been produced in line with the Information Commissioner's CCTV Code of Practice and the Home Office's Surveillance Camera Code of Practice.

Throughout this document the term 'Authority' is used to represent both the legal status of West Yorkshire Fire and Rescue Authority and the operational status of West Yorkshire Fire and Rescue Service.

2 Purpose of the Scheme

WYFRS own and operate CCTV systems for the purpose of:

a) Fixed installation CCTV systems:

- Reducing crime in the form of theft, fire, vandalism, physical and verbal abuse to its personnel and property by aiding prevention through deterrence and detection
- Providing 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
- Maintaining the security of its buildings and associated contents
- To obtain evidence for use in the investigation of criminal actions, serious breaches of health and safety legislation and serious breaches of WYFRS disciplinary procedures (subject to conditions, see *)

b) CCTV systems mounted on fire appliances (Silent Witness):

- Reducing 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
- Reducing 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
- To obtain evidence for use in the investigation of criminal actions, serious breaches of health and safety legislation and serious breaches of WYFRS disciplinary procedures (subject to conditions, see *)
- Providing a training knowledge pool to offer good learning experiences and improvements in operational tactics and command
- Promoting community safety and education utilising the Media

c) Mobile and Body Worn Video Cameras (BWVs) including Unmanned Aerial Vehicles (UAVs):

- To help meet the statutory duty under the Civil Contingencies Act 2004 to maintain operational functionality and interoperability with other responders at all times
- Provide real-time images from unmanned aerial vehicles (UAVs) tri-pod mounted and body-worn cameras to enable faster, more effective command decisions.

The use of CCTV for any other purpose may be unlawful and may bring the system into disrepute. This may result in any subsequent case being discontinued at court and a civil claim being lodged.

**The Authority will only use CCTV footage for use in a staff disciplinary case when there are reasonable grounds to suspect gross misconduct (such as a complaint or information received) and not for the investigation of minor procedural infringements or misdemeanours or to generally monitor staff activity.*

In these situations the investigating officer will formally request access to images using the Access to Images Request procedure (see Appendix A), where these may prove or disprove suspected potential gross misconduct. Where access is granted, the confidentiality of these images and who is able to access them will be closely controlled.

3 Responsible persons

The following posts have the appropriate responsibility as indicated:

a) The Information Management Officer is responsible for managing the day to day requests for information covered by the Data Protection Act 1998 and Freedom of Information Act 2000
b) The Service Standards Officer is responsible for managing the Complaints Procedure
c) Responsibility for day to day operations of the different CCTV systems will fall within the responsibilities of the nominated persons (Property Manager, Visual Services Supervisor, Transport and Logistics Manager, Operational Crew and Watch Commanders (Silent Witness) and the OIC Command Unit (Mobile/BWV)).

The responsible persons will annually:

- Review documented procedures to ensure that the provisions of the applicable Codes of Practice are being complied with
- Compare the CCTV database application with the hard drives access record to ensure no unauthorised access has taken place
- Sample recorded images to ensure the equipment is being used for its intended use only
- Monitor the quality of the maintenance work.

4 Covert recording

This Policy does not cover covert surveillance activities including core statutory functions as they are covered by the Regulation of Investigatory Powers Act (RIPA) 2000.

Covert surveillance is that which is carried out in a manner calculated to ensure that subjects of it are unaware it is, or may be taking place. Any such covert monitoring will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring, and only for a specific unauthorised activity. Refer to the RIPA Policy and Procedures and the Employee Monitoring Policy for further details.

Any use of this CCTV system or materials produced which contravenes this policy (i.e. for private or unauthorised purposes) may result in disciplinary action for cases considered to be misconduct/gross misconduct.

5 Signage

In accordance with the Information Commissioner's CCTV code of practice, appropriate signs must be displayed where CCTV is operating.

All WYFRS buildings/premises and vehicles fitted with CCTV systems will prominently display public awareness signs detailing:

- West Yorkshire Fire and Rescue Authority is responsible for the CCTV scheme (unless it is otherwise obvious)
- CCTV equipment in operation (including the use of audio recording where relevant)
- Purpose of the CCTV system
- Contact telephone number

6 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 (RIPA)
- European Convention of Human Rights
- Freedom of Information Act 2000

The fixed installation 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 WYFRS personnel and any member of the public with lawful reason for being within the grounds or premises of Fire Service property.

All proposed new installations of fixed installation of CCTV equipment (including extensions to existing networks) will need the approval of the Director of Service Support.

The use of fixed installation 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 installation CCTV system will not be used for anticipated targeted surveillance.

6.1 The siting of Fixed Installation CCTV Systems

The fixed CCTV surveillance system will continuously capture imagery from cameras for up to 24 hours per day. The fixed cameras will capture designated surveillance areas.

The following standards must be adhered to:

1. After installation, make an initial check of the equipment to ensure it works properly.
2. Ensure that tapes or discs, where used, are of good quality.
3. Do not continue to use media once it becomes clear that the quality of the images has begun to deteriorate.
4. Where the location of the camera and time/date are recorded, these should be accurate. Document the system for ensuring accuracy.
5. Site the cameras so they will capture images relevant to the purpose(s) for which the scheme has been established.
6. Cameras should be properly maintained and serviced and maintenance logs kept.
7. Protect cameras from vandalism so that they are kept in working order.
8. In the event that cameras break down or are damaged, there should be clear responsibility for getting them repaired and working within a specific time period.

6.2 Training

Operators

Appropriate training will be provided in accordance with the Information Commissioner's CCTV Code of Practice 2008 and the Home Office's Surveillance Camera Code of Practice 2013.

The Property Manager (or designate) 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 premises.

Nominated staff who are to operate the system will be identified by line managers.

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

- The purpose of the scheme
- Rights of individuals under the CCTV system
- Information Security Policy
- Data Protection / Freedom of Information Policy
- Equipment use
- Recognition of the privacy implications of the visual area to be covered
- Recognition that images must only be viewed by authorised employees of the Authority.

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

6.3 Maintenance

The overall maintenance of the system will be the responsibility of Property Management Unit. The Authority's fixed installation cameras have a maintenance contract. The maintenance of CCTV will be undertaken by an approved contractor.

The operators will check the equipment on a daily basis to ensure performance and reliability by the viewing of live recorded imagery. The nominated person will be informed of any malfunction/unsatisfactory performance and will inform the appropriate individuals in accordance with equipment maintenance procedures.

All servicing and maintenance on the system must be recorded/documented onto a maintenance log.

7 Fire Appliance (Silent Witness) CCTV

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

- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)
- 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 Authority personnel and any member of the public with lawful reason for being at that location when the Authority is operating in the community.

7.1 The Siting of Vehicle Mounted CCTV Systems

The vehicle mounted CCTV surveillance is activated by the Watch Commander/ Crew Commander of the applicable fire appliance. There are either two or four cameras on each appliance:

- One camera is mounted on the rear of the appliance facing backwards
- One camera is mounted on the dashboard in the cab in front of the driver's position facing forwards.
- For appliances that have four cameras fitted there is also one camera positioned on each of the left hand and right hand side of the vehicle.

The system also includes an audio recording function with a microphone positioned in the cab of the vehicle. This function is activated upon the operation of the Silent Witness CCTV system.

In siting and maintaining the CCTV equipment the Authority will ensure that:

- The location of cameras is justified by the stated purpose as outlined in the vehicle mounted CCTV scheme
- The equipment should as far as practicable and possible, continually operate effectively and efficiently
- The image quality is maintained on the reproduction to CD/DVD
- 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 Transport and Logistics Manager or their designate, should be recorded.

For further details relating to the operational use of the Silent Witness Camera system refer to Operational Procedure No 53

8 Mobile and Body Worn Video (BWV) CCTV Systems including Unmanned Aerial Vehicles (UAVs)

Mobile and Body Worn Video (BWV) are deployed from the Command Unit at all six pumps and above incidents. The systems are utilised to ensure that all commanders share the common operational picture of what is happening on the ground. Gold, Silver and Bronze Commanders are able to make better-informed decisions if they all have access to the same critical information – information that is not only accurate, but is also current and relevant to the situation in hand.

8.1 Procedures for using Mobile and BWV CCTV

Whilst the primary purpose of deploying and operating mobile and BWV devices is to capture incident footage it cannot be ruled out that the images of third parties (e.g. members of the public) may be captured during any recording. In order to comply with our responsibilities under the Data Protection Act the following rules must be followed:

- All users must wear full uniform and deploy the equipment in the correct and approved overt manner
- When recording is taking place the Command Unit external digital messaging system will be utilised to display that CCTV recording is occurring. Pop-up signage will also be deployed in the immediate vicinity to advise individuals (subjects) that recording is taking place
- If possible, depending on the circumstances, a verbal warning should be given that recording is about to commence
- It must be ensured that:
    - Any recording is in the interests of the incident command and/or the safety of the operational crew or members of the public
    - The recording is not covert

    - The system is not recording all the time for no acceptable reason
- Once recordings have commenced at a given incident the recording, where practicable, should continue uninterrupted until the incident is concluded. Should any recording be discontinued for any reason prior to the conclusion of the incident (i.e Officer/Staff Safety), the reason must be recorded in any subsequent statement or contemporaneous note.

9 Recorded Image Security

Access to recorded images on the hard drive will only be made after the appropriate authorisation is given. Refer to section 11 and Appendix A of this policy for further details.

Access to recorded images on the hard drive is restricted to the trained team nominated under the direct control of the Property Manager or Visual Services Supervisor.

All access to the recorded images shall be recorded in the Access to Images log maintained by Corporate Services.

All recorded images accessed and downloaded on to CD/DVD will be given a unique reference number.

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 whilst viewing is taking place.

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

- The date and time of removal
- The name of the person removing the images
- The name(s) of the person(s) viewing the images. If this should include third parties, include the organisation and/or role of that third party
- The reason for the viewing
- The outcome, if any, of the viewing
- 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.

10 Retention of Recorded Images

Images and recording logs will be held in accordance with the Authority's Records Retention Schedule and associated schedules.

For digital recording systems, CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and in any event, will not be held for more than 30 days, without prior authorisation by a Director for reasons which are recorded and notified to the Information Management Officer (IMO). Images stored on removable media such as CD/DVDs will be erased or destroyed once the purpose of the recording is no longer relevant. All digital recordings will be digitally watermarked to maintain integrity.

Recording media no longer in use will be securely destroyed.

11 Access to and disclosure of images

Access to, and disclosure of, images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are retained, and also ensure that the images can be used as evidence if required. Images can only be disclosed in accordance with the purposes for which they were originally collected, and in accordance with the Authority's Data Protection Notification to the Information Commissioner's Office.

The Authority's Data Protection Policy, Visual Imaging Policy and Operational Procedure No. 53 should also be consulted in relation to the capture, storage, access to and disposal of personal information - in this case images and/or audio.

The specific details of how to request access to CCTV images is covered at Appendix A of this policy.

This document separates access and disclosure into the following subsections.

11.1 Subject Access Requests

Under the Data Protection Act 1998 individuals have a right to view any recorded images of themselves and, unless they agree otherwise, to be provided with a copy of the images. Any Officer who receives such a request should immediately forward the request, known as a Subject Access Request, to the Information Management Officer who will require a copy of the recorded images and will coordinate a response to the request. A response is required to be provided to the applicant within 40 calendar days of receiving a valid request and the Authority can charge a fee of up to £10.

The applicant must make their subject access request in writing (or electronic means) using the form that can be found on our website www.westyorksfire.gov.uk/data-protection or by writing to:

Information Management Officer
West Yorkshire Fire and Rescue Service
Oakroyd Hall
Bradford Road
Birkenshaw
West Yorkshire
BD11 2DY
Email: information@westyorksfire.gov.uk

When an applicant makes a subject access request for CCTV or other video images it is necessary for them to provide:

- Proof of their identity
- A clear description of the location in which they believe they were recorded on CCTV, along with the date and time
- A clear picture of themselves, to aid identification and enable a comparison with CCTV footage
- Ideally a description of what they were wearing at the time the images were captured
- The £10 fee as appropriate.

Once it can be confirmed that the applicant is the individual on the CCTV image the applicant will be asked whether they choose to simply view the CD or to receive a copy.

If images of third parties are also shown with the images of the applicant, consideration must be given to whether it is necessary to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. In many cases, images can be disclosed as there will not be such intrusion.

11.2 Freedom of Information Act

Under the Freedom of Information Act 2000 (FOIA) individuals have the right to request recorded information the Authority holds. Such requests are coordinated by the Information Management Officer and must be responded to within 20 working days of receipt of the request. Section 40 of the FOIA exempts information about individuals from being disclosed.

If a request for CCTV footage is received, the following points should be considered:

- Are the images those of the requester? If so then that information is exempt from the FOIA. Instead this request should be treated as a Data Protection Subject Access Request as explained above.
- Are the images of other people (third parties)? These can only be disclosed if disclosing the information in question does not breach the data protection principles.

In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to an FOI request as the applicant could potentially use the images for any purpose and the individual concerned is unlikely to expect this. This may constitute unfair processing in breach of the Data Protection Act (DPA).

However, footage exempt from FOIA should be considered on a case-by-case basis as it may be lawful to provide it without breaching the DPA, where the reason for the request is taken into account, as indicated earlier.

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

- A copy of the CCTV Code of Practice
- A copy of the Freedom of Information Policy or Data Protection Policy which detail the relevant request process
- The complaints procedure to be followed if they have concerns about the use of the system or about non-compliance with the provisions of the CCTV Code of Practice.

11.3 Access to and Disclosure of Recorded Images to Third Parties

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it will not be appropriate to disclose images of identifiable individuals to the media for identification purposes; this should not be done by anyone other than a law enforcement agency.

Disclosure of the recorded images unedited or edited may be made where the images are required for:

- National security – however, a certificate of exemption, signed by a Minister of the Crown, is conclusive evidence of the fact that the images are required for safeguarding national security;
- Crime and taxation purposes - this will happen where information is required for:
  - the prevention and detection of crime; or
  - the apprehension or prosecution of offenders; or
  - the assessment or collection of any tax or duty; or
  - any imposition of a similar nature.
- Where disclosure is required by law including an order of a court;
- Disclosure is made in connection with legal proceedings.

The Chief Legal and Governance Officer must be consulted whenever a request for any of the above reasons is received.

11.4 Access to and Disclosure of Images for Media, and Equipment Evaluation

Images recorded by the system may be used for media and equipment evaluation purposes. Since the system will be indiscriminate in the recording of data it may be necessary to edit some 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.

12 Requests to prevent the processing of data

All requests from individuals must be passed to the Information Management Officer who will ensure a decision is made whether the request will be complied with or not when it relates to:

- Preventing processing likely to cause substantial and unwarranted damage to that individual
- Preventing automated decision taking in relation to that individual

The Information Management 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 Information Management Officer shall document:

- The decision
- The request from the individual
- Their response to the request from the individual.

Appendix A - How to Request CCTV Images

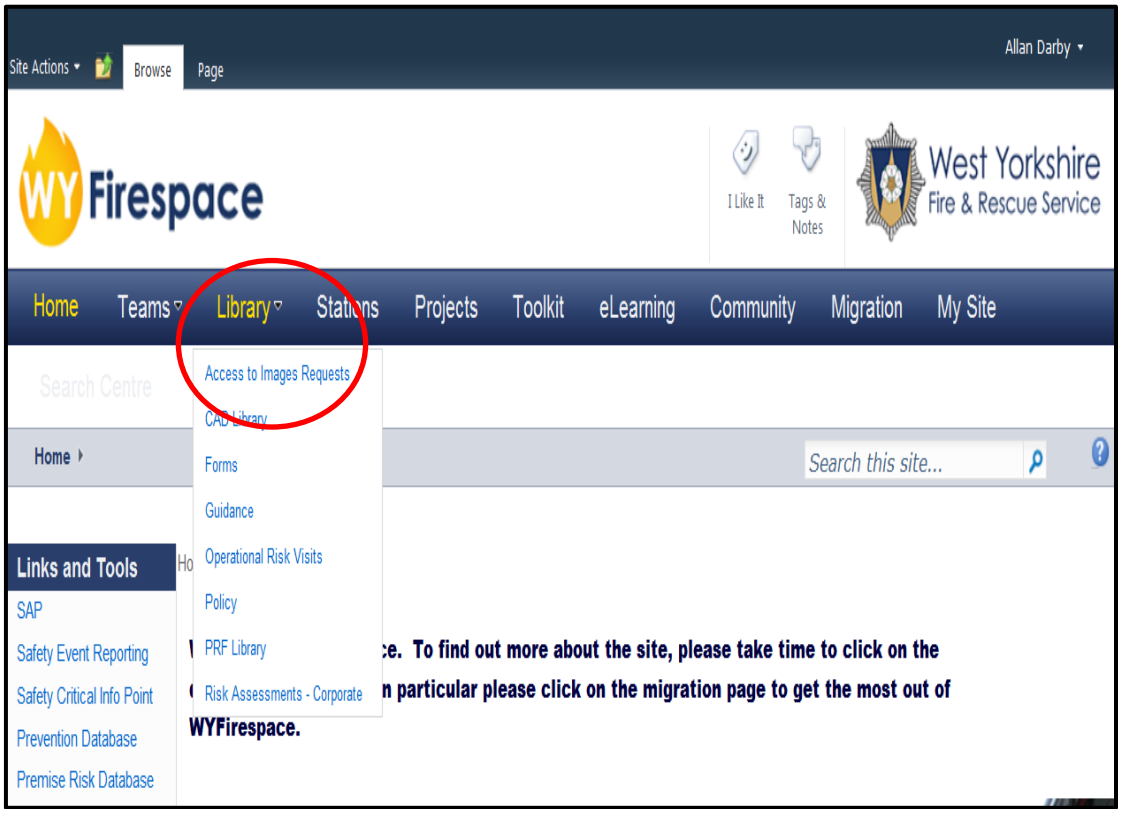
How to request Video images

If there is a requirement to access any video images captured on any WYFRS video capture device eg Fixed Camera CCTV, Silent Witness footage or Body Worn Video/Mobile Video Cameras the following procedure should be followed in accordance with the Closed Circuit Television (CCTV) Policy (CS-POL005).

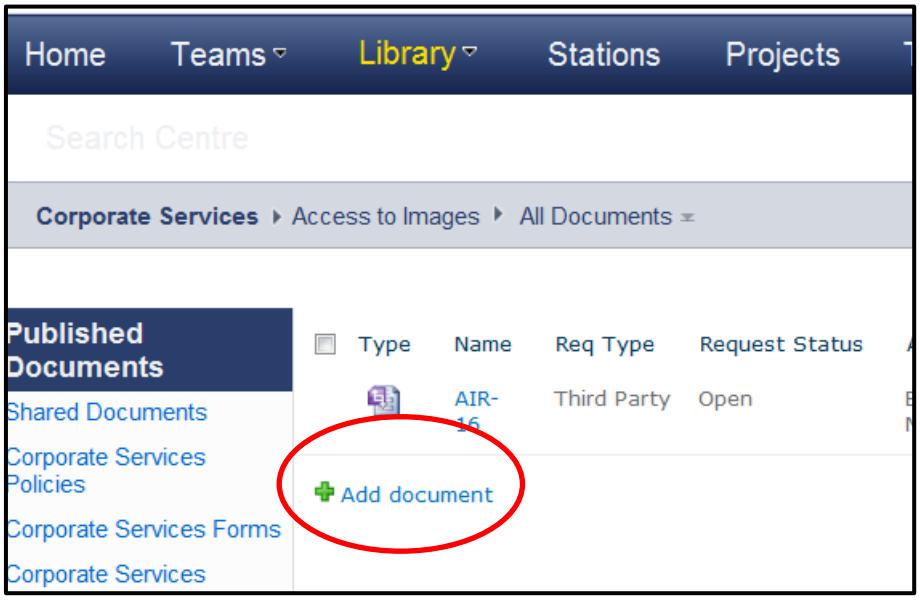
To ensure availability of images any requests for disclosure should be submitted as soon as possible after the incident or event. If there are any delays with submitting the request the availability of the images cannot be guaranteed as this is dependent on the retention periods and fire appliance activity.

Requests from staff in relation to work activity/investigations

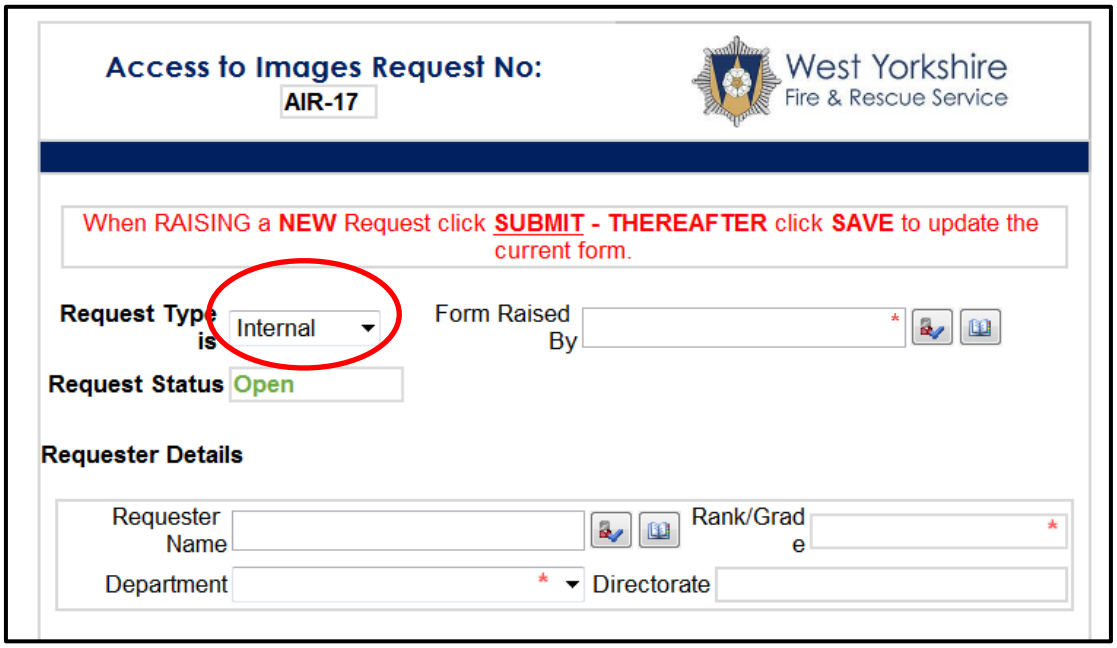
- The Access to Images request form (Form 706) is accessed from the Library drop down menu on the top tool bar of the WYFirespace should be completed – see Closed Circuit Television (CCTV) Policy (CS-POL005) for further details.



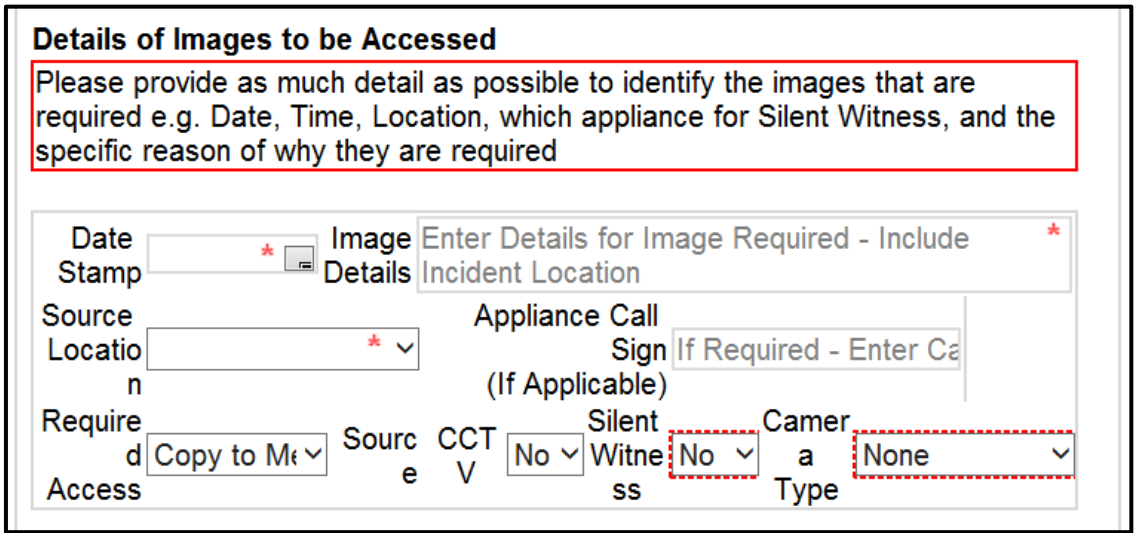
- This will open up the Access to Images list and you will need to select 'Add document' to create a new form.



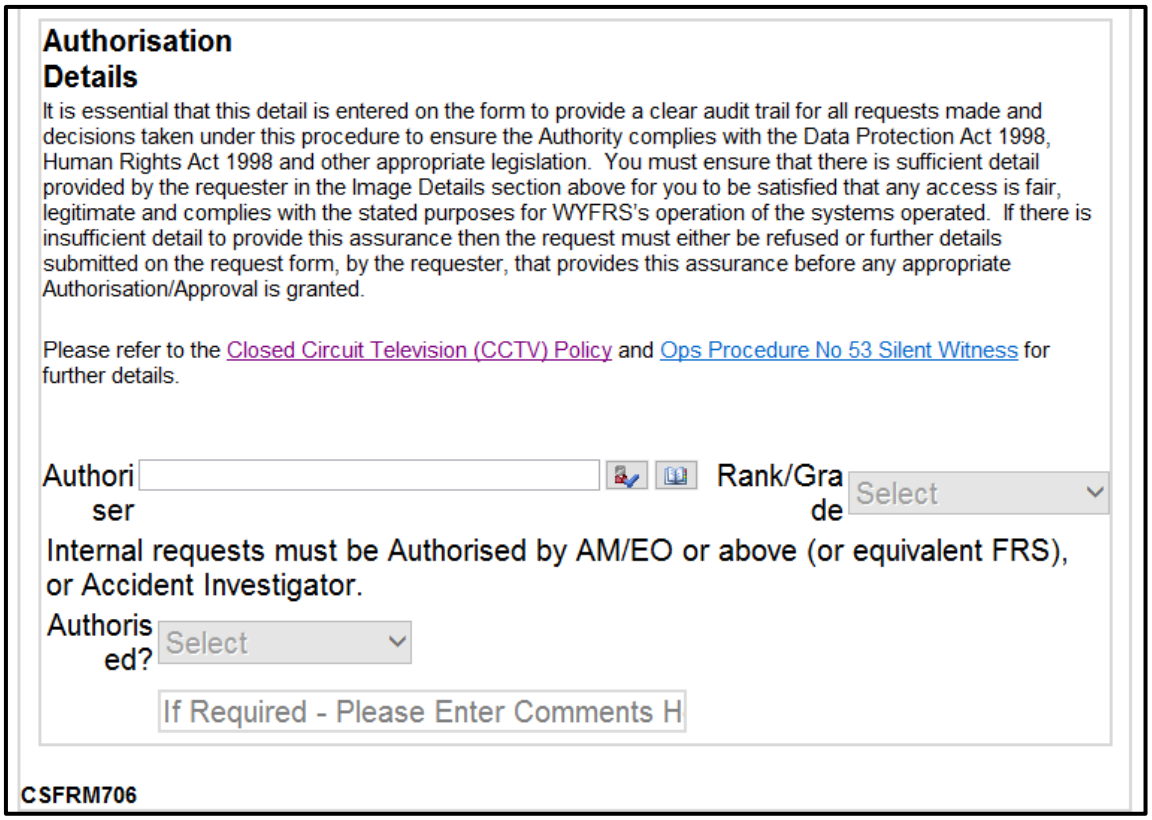
- The form will automatically generate a Request Number (AIR-***). You will need to fill in all of the appropriate fields with the 'Request Type' selected as 'Internal' and clearly stating the details relating to person making the request.



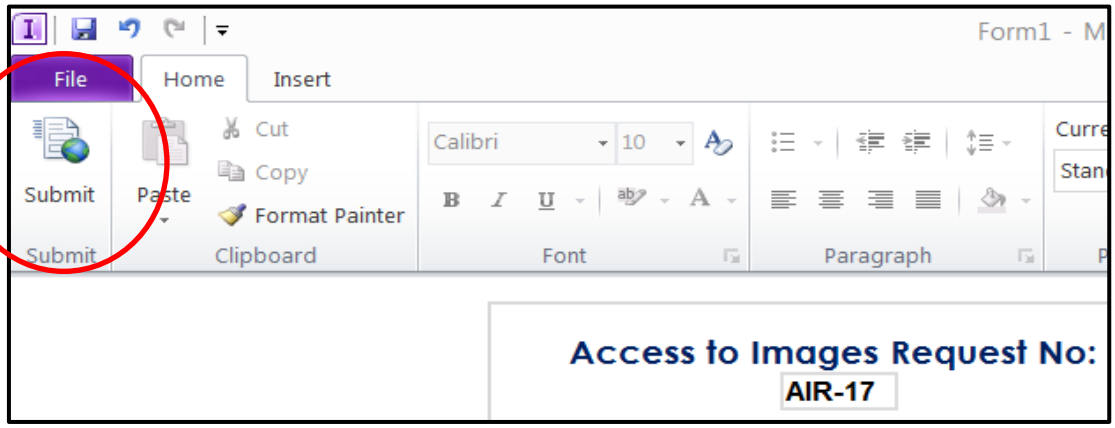
- The details of the Images to be Accessed and the reason for the request should be completed with the specific details and the appropriate access requirement selected (either 'View Only' or 'Copy to Media'). At least one 'Video Source' should be selected as appropriate.



- The request must be authorised for disclosure by the appropriate Area Manager/Senior Manager of the person making the request. If the appropriate manager is not available and for matters of urgency then an alternative Area Manager/Senior Manager may authorise the request (if the images are required for Fire Investigation or Accident Investigation purposes the designated Station Managers will have the authority to authorise the request and will be the only exception to this rule).



- Once these details have been entered press the 'Submit' button on the left of the top tool bar. This then sends the form by workflow for authorisation to the appropriate manager.



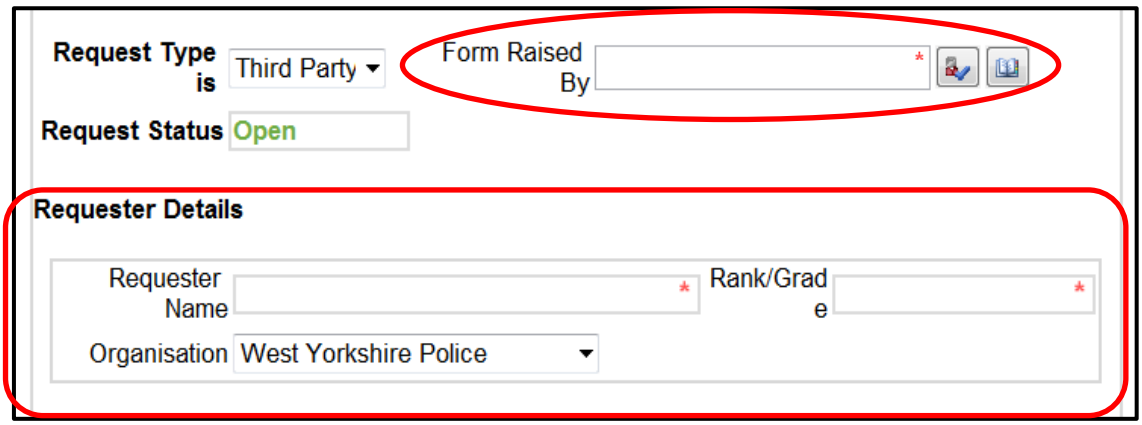
- Once the manager has authorised the disclosure the workflow will direct the request to Property Management Unit, Visual Services and/or OIC Command Unit, as appropriate, who will arrange the data transfer to CD/DVD according to continuity of evidence requirements. The requester will be then notified when the images are available for viewing/collection.

Request from the Police, Law Enforcement or National Security Agencies

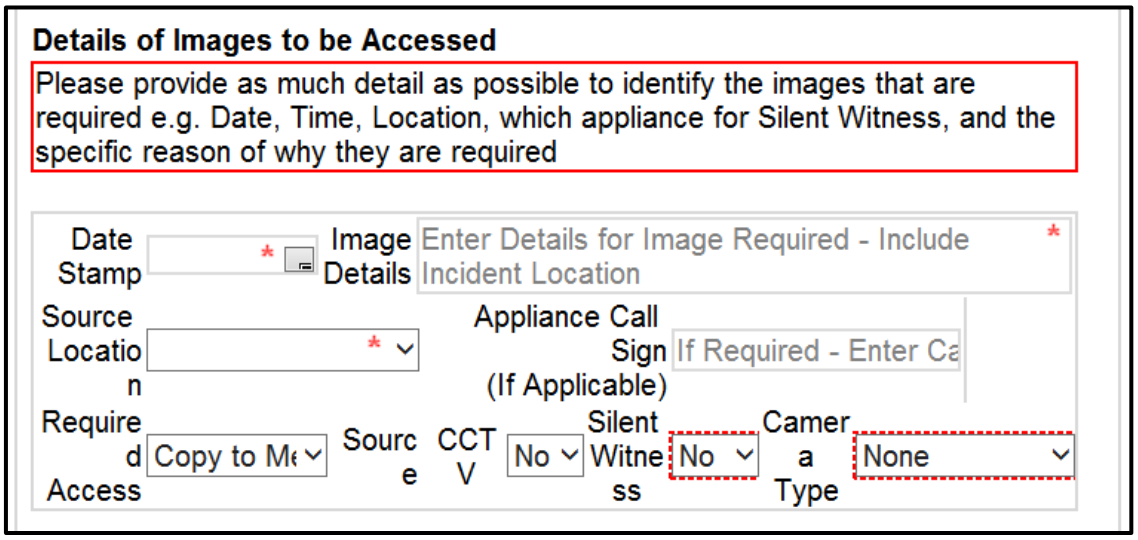
These requests must be made on the Access to Images request form (Form 706) accompanied by a Section 29 Notice (also known as a DP7 Form within the Police service). The Section 29 Notice (or DP7 Form) must be signed by an Inspector or above or relevant Senior Manager.

- The process is largely the same as above but the 'Request Type' should be selected as 'Third Party'.

- The 'Form Raised By' should be the individual who receives the Section 29 Notice or DP7 Form and the 'Requester Details' should be the external person making the request eg a police officer.

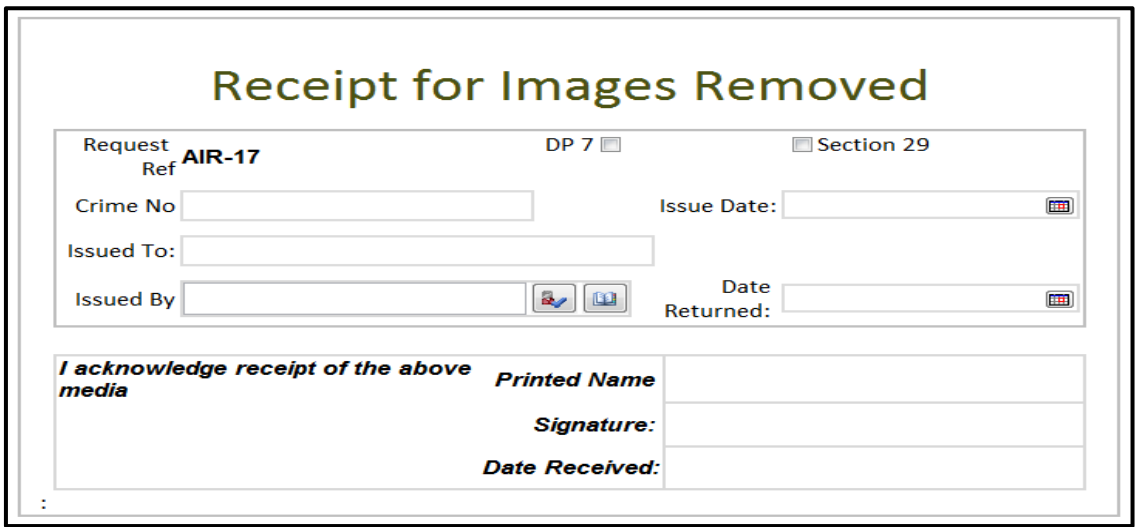


- The details of the Images to be Accessed and the reason for the request should be completed with the specific details and the appropriate access requirement selected (either 'View Only' or 'Copy to Media'). At least one 'Video Source' should be selected as appropriate.



- Once the appropriate details have been entered and the form submitted the workflow will direct the form for Disclosure Approval. **The Chief Legal and Governance Officer, or designated officer, is the only individual who can authorise disclosure of information to the police or law enforcement agencies under Section 29 of the Data Protection Act 1998.**

- If Disclosure Approval is granted the form will automatically be forwarded to Property Management Unit, Visual Services or OIC Command Unit as appropriate who will arrange the data transfer to CD/DVD according to continuity of evidence requirements. The requester will be then notified when the images are available for collection and a Receipt for Images must be signed by the individual collecting the CD/DVD.

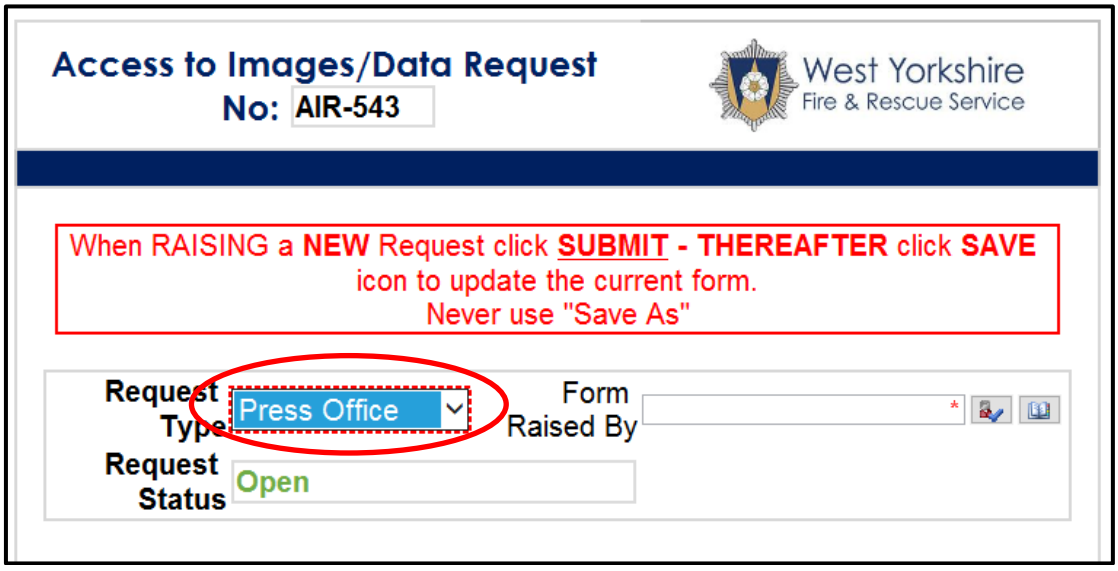


Requests made out of hours

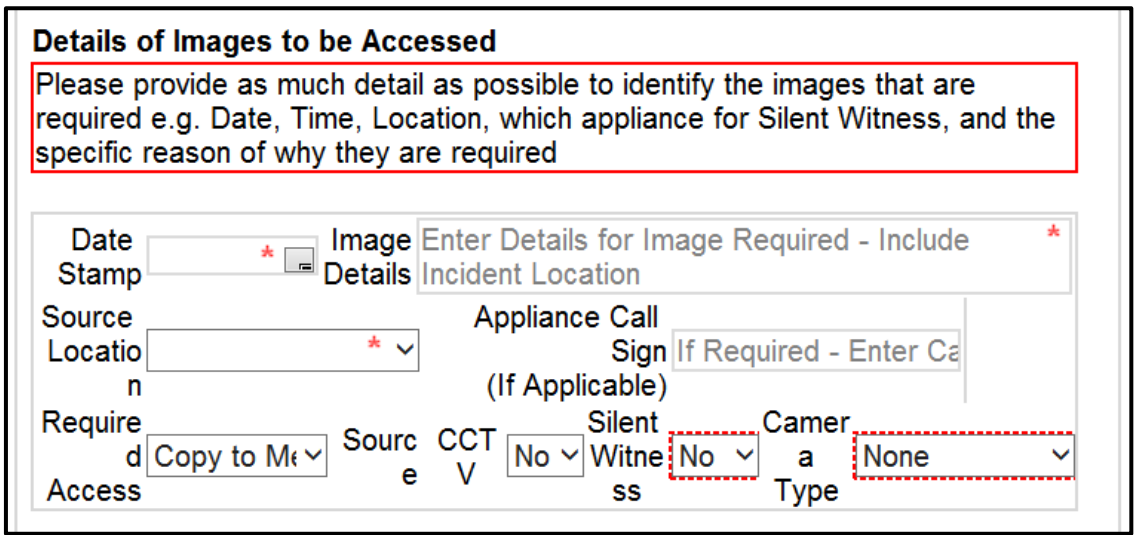
Where requests are made out of 'normal' working hours and are required immediately Control will contact the First Call Area Manager or Group Manager, who will have overall responsibility for authorising the retrieval of the hard drive. The data transfer to CD/DVD will be dealt with during normal office hours according to continuity of evidence requirements detailed above.

Requests from the Public Information Team in relation to release of video footage to the media

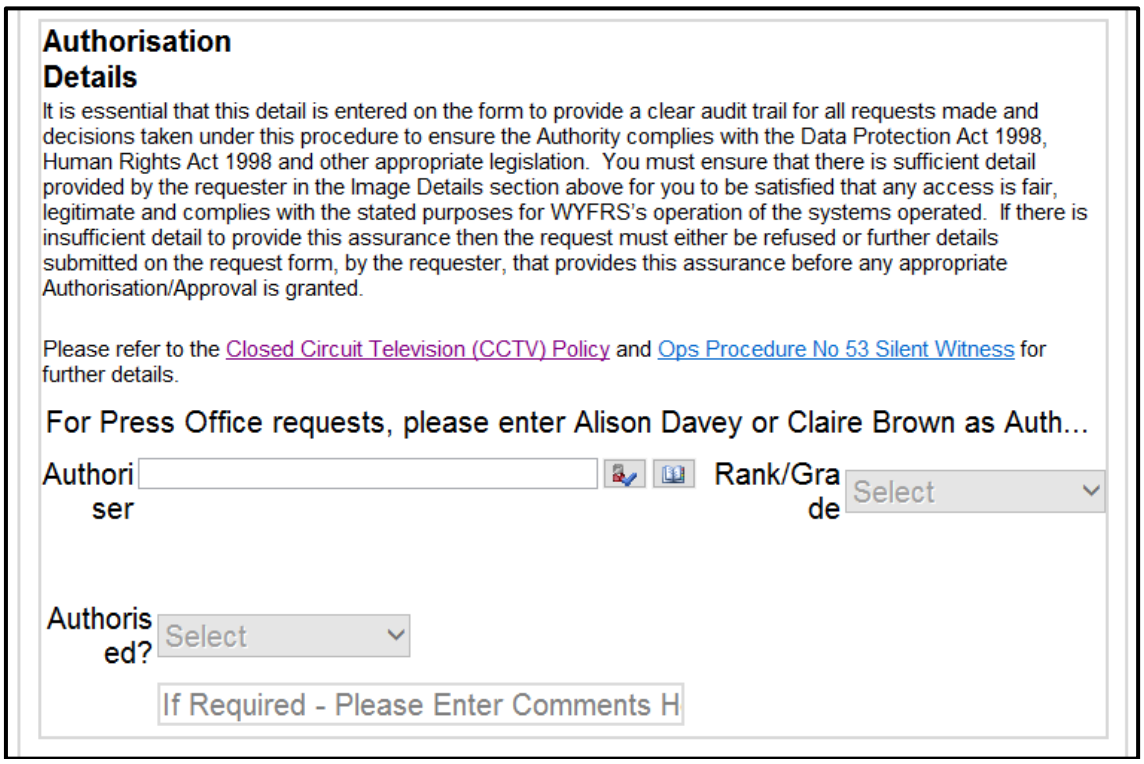
These requests are made using the same Access to Images Request form (Form 706) and selecting the 'Press Office' option from the drop down menu.



- The details of the Images to be Accessed and the reason for the request should be completed with the specific details and the appropriate access requirement selected (either 'View Only' or 'Copy to Media'). At least one 'Video Source' should be selected as appropriate.

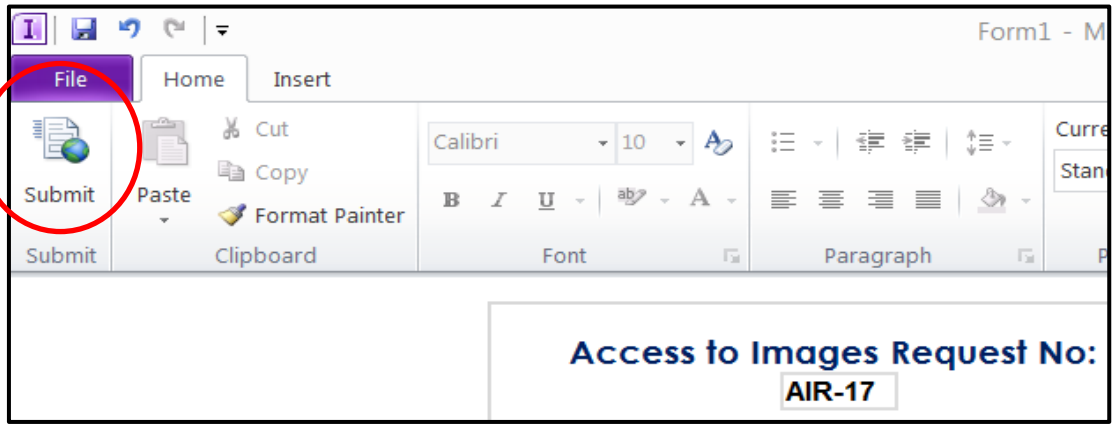


- The Authoriser should be entered who will assess the request for appropriateness for the intended use.



- An operational Area Manager must be inserted who will view the selected footage to ensure that it does not identify any areas of operational malpractice that would not be appropriate for external disclosure.

- Once these details have been entered press the 'Submit' button on the left of the top tool bar. This then sends the form by workflow for consideration and approval in respect of the legal responsibilities regarding such external disclosures.



- If Disclosure Approval is granted the form will automatically be forwarded to Property Management Unit, Visual Services or OIC Command Unit as appropriate who will arrange the data transfer to CD/DVD according to continuity of evidence requirements. The Public Information Team will be then notified when the images are available for collection and a Receipt for Images must be signed by the individual collecting the CD/DVD.

Requests from members of the public

- Any requests from members of the public to access images of themselves as the subject or of other individuals (third parties) must be forwarded to the Information Management Officer, Corporate Services who will deal with it as Data Protection Act Subject Access Request or Freedom of Information Act Request as detailed in Section 9 of the Closed Circuit Television (CCTV) Policy (CS-POL005).
- The Information Management Officer or the Corporate Services Manager will consult with legal services if required
- On receiving disclosure approval the Property Manager or Visual Services Supervisor (or the nominated representative) will arrange the data transfer to CD/DVD according to the continuity of evidence requirements
- Requests from members of staff relating to access to images that constitute their own personal information will be dealt with as a Subject Access Request in accordance with the Data Protection Policy (CS-POL008).

Applicable to all requests

All requests for access or disclosure of video images shall be recorded in the Access to Images log, which is held securely with restricted permissions and managed by Corporate Services.

No disclosure shall be made until the images are viewed by the Property Manager/Visual Services Supervisor (or nominated representative) to ensure the Authority is not compromised by the disclosure. If third party images are not to be disclosed, the images must be disguised or blurred prior to the release of the footage.