



# Closed Circuit Television (CCTV), Video and Audio Recording Equipment and Vehicle Data Devices

This document is uncontrolled when printed. All users are responsible for checking to confirm that this is the current version before use.

**PREVENTING PROTECTING RESPONDING**

Version: 1	Next review: 03/01/2019	Closed Circuit Television (CCTV), Video and Audio
Status: Awaiting Review	Issue date: 03/01/2018	Recording Equipment and Vehicle Data Devices

Uncontrolled when printed – check on line to check latest version



## Contents

1	Introduction.....	3
2	Purpose .....	4
2.1	Mobile CCTV & data recorders.....	4
2.2	Fixed installation CCTV on all AF&RS premises .....	4
3	Scope .....	5
4	Responsibility .....	6
5	Mobile CCTV audio & data recorders .....	7
5.1	Location and positioning of the cameras .....	7
5.2	Responsible persons .....	7
5.3	Operational Guidance.....	8
5.4	Local Area Network (LAN) link.....	8
5.5	Image storage, retention and deletion .....	8
5.6	Training for operating the equipment.....	9
6	Fixed Installation CCTV.....	9
6.1	Location and positioning of the cameras .....	9
6.2	Responsible Persons.....	10
6.3	Procedure.....	11
6.4	Image storage, retention and deletion .....	11
6.5	Training .....	11
6.6	Maintenance.....	12
7	General Signage .....	13
8	Data Security.....	13
9	Requesting copies of CCTV images, audio and data .....	14
9.1	Freedom of Information Act .....	15
9.2	Requests from agencies and other organisations.....	16
9.3	Internal AF&RS staff requests for copies of CCTV/audio data .....	17
<b>9.4</b>	<b>Other requests regarding the processing of personal data.....</b>	<b>17</b>
10	Appeals and Complaints .....	18

### PREVENTING PROTECTING RESPONDING

Version: 1	Next review: 03/01/2019	Closed Circuit Television (CCTV), Video and Audio
Status: Awaiting Review	Issue date: 03/01/2018	Recording Equipment and Vehicle Data Devices

Uncontrolled when printed – check on line to check latest version



## 1 Introduction

Avon Fire & Rescue Service (AF&RS) own and operate Closed Circuit Television (CCTV) and vehicle telematics in order to provide a safe and secure environment for staff and visitors, the public, and to protect our property and assets.

In order to do this AF&RS may use Closed Circuit Television (CCTV) and vehicle telematics in the following situations:

- On our fire appliances
- At our premises,

We recognise that the use of CCTV and vehicle telematics means that we may collect personal data about individuals.

This document sets out the accepted use and management of the CCTV equipment and images, vehicle telematics and the data it produces to ensure that AF&RS complies with the following legislation:

- The Data Protection Act 2018 - DPA;
- The EU General Data Protection Regulations 2016 - GDPR
- Human Rights Act 1998;
- The Regulation of Investigatory Powers Act 2000 (RIPA);
- The European Convention on Human Rights; and
- All other applicable legislation.

This document has been produced in line with the standards detailed in the [Information Commissioner's CCTV Code of Practice](#) and the [Home Office's Surveillance Camera Code of Practice](#).



## 2 Purpose

AF&RS own and operate CCTV systems and vehicle telematics to support staff safety, security of our staff and assets and for the purpose of accident / incident investigation. Data and images recorded may also be used for operational training, evaluation of equipment, and the promotion of community safety (any use is subject to data protection legislation).

### 2.1 Mobile CCTV & data recorders

The data recorded on mobile CCTV and data recorders mounted on AF&RS vehicles will be used for:

- Supporting accident and incident investigations involving AF&RS activities in accordance with the Health Safety Welfare (HSW) Standard Operating Procedure (SOP) 5 Accidents and Incidents
- Supporting the development of driver training as part of a programmed training event
- Identifying driving techniques for accident/incident reporting and programmed training
- Identifying engine emissions, fuel consumption, vehicle mileage and driving hours
- Reducing crime and anti-social behaviour towards staff, by aiding prevention through deterrence and detection. Such recordings may be used as evidence against the perpetrators of such behaviour
- Fire Investigation (FI)
- Providing a pool of learning experiences for training purposes which will assist in improving operational tactics and command
- Promoting community safety and education (any use will be subject to data protection legislation)
- Reducing insurance claims and associated insurance premiums where possible

### 2.2 Fixed installation CCTV on all AF&RS premises

- To reduce crime and anti-social behaviour towards AF&RS staff, visitors and to protect our property and assets by aiding prevention through deterrence and detection
- Provide a safer and a more secure environment for all staff and visitors 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
- Support accident and incident investigations involving AF&RS property

AF&RS also recognise that in the event of conducting a staff investigation, it sometimes may be necessary to access recordings and images taken by the above equipment. Such instances will only be carried out in a controlled manner by an appointed Investigation Officer with prior written authorisation by a member of the Service Management Board.



### 3 Scope

Throughout this document the term 'Avon Fire & Rescue Service (AF&RS)' is used to represent both the legal status of Avon Fire Authority (AFA) and the operational status of Avon Fire & Rescue Service.

The scope of this policy relates to the use of CCTV and related media equipment by AF&RS. This will assist our function for the purposes of preventing, protecting and responding by improving performance, knowledge and understanding of our activities, and protecting our assets. The operation of equipment detailed in this policy will only be used overtly (open) and we will provide clear signage and /or communications when such equipment is in operation to maintain transparency.

In terms of who, the scope of this policy extends to the following:

- All AF&RS staff
- Visitors to our premises
- Contractors/suppliers
- General public (where overtly captured/recorded)
- Anyone requesting to view recorded images, audio and telematics data, to include internal staff, members of the public and other agencies such as the police.

In terms of what is covered:

- Fixed premises CCTV, appliance mounted CCTV and data recording boxes (telematics) and any similar equipment
- The capture and storage of data (using mobile media and the AF&RS network)
- Access to images and any recorded data
- Internal and external requests for images and recorded data are processed in line with current data protection legislation and any other related legislation

The following AF&RS internal policies are to be used in conjunction with this policy:

- Data Protection Policy
- Freedom of Information Policy
- Information Security Policy
- IT Systems Acceptable use Policy
- Laptop and Mobile Device Policy
- Removable Media Policy
- Social Media Policy
- HSW SOP 5 Accidents and Incidents



## 4 Responsibility

AF&RS is responsible for the CCTV scheme (unless it is otherwise obvious). AF&RS will ensure that the following statutory requirements are complied with for the use of CCTV equipment and images and vehicle telematics and the data produced.

Whilst the primary purpose of operating the various modes of CCTV and associated equipment for the reasons stated in Section 2 'Purpose' of this policy, it cannot be ruled out that the images of third parties (e.g. members of the public) may be captured during any recording.

AF&RS has a legal responsibility as the data controller under the data protection legislation and will operate all CCTV, audio and data recording systems in accordance with the [Information Commissioner's CCTV Code of Practice](#).

**Overall responsibility** for the AF&RS CCTV and related equipment resides with the Fire Authority.

**The Chief Fire Officer** will ensure that suitable resource is allocated for the provision and the secure use of the equipment, and that staff are trained appropriately.

**The Senior Information Risk Owner (SIRO)** is a member of the Service Management Board (SMB) and ensures that the Fire Authority, CFO and the SMB are fully aware of the status of information risk. SMB members ensure that appropriate mitigating actions are implemented across the Service.

**Assistant Chief Fire Officer (ACFO) for Service Delivery** has overall responsibility regarding the commissioning of this policy and any future updates.

**The Data Protection Officer (DPO)** will provide guidance regarding the Data Protection Act 2018, EU General Data Protection Regulations (GDPR) 2016, and Freedom of Information Act 2000 requirements concerning the use of the CCTV and associated equipment, and development of this policy. The DPO and the Data Protection Team will also manage internal and external requests for copies of personal information held by AF&RS, which will include any requests for personal data captured by this equipment.

**The Director Legal & Corporate Services** will have responsibility for the procurement process in line with the 'Avon Fire Authority Standard Terms and Conditions for the supply of Goods, Works and/or Services' and any framework agreement that we participate in for the supply of the equipment and that chosen supplier/s possess the correct industry approved accreditations.

### PREVENTING PROTECTING RESPONDING

Version: 1	Next review: 03/01/2019	Closed Circuit Television (CCTV), Video and Audio
Status: Awaiting Review	Issue date: 03/01/2018	Recording Equipment and Vehicle Data Devices



## 5 Mobile CCTV audio & data recorders

### 5.1 Location and positioning of the cameras

Vehicles fitted with mobile CCTV and data recorders will display signage to advise that CCTV cameras are in use. These signs will comply with the current legislation and guidance supplied by the Information Commissioner.

The vehicle cameras will:

- face outwards from the appliances
- be static with no facility to move, tilt or re-direct the camera angles
- be positioned on the front, sides and rear of the appliance
- have infrared night vision capability
- will automatically record the date, time, vehicles speed and location by using the Global Positioning System (GPS),
- any images captured will record High definition (HD) quality

The vehicle cameras may have audio capability, which will be turned off by default on all appliances. There are, however, exceptional circumstances on individual appliances where the use of audio may be necessary. Before audio is activated, valid reasons must be identified and prior approval will be sought from a member of SMB, which will be documented.

Staff will be made aware of this decision prior to activation and this can only be activated in advance by an authorised user. Such instances where this would be necessary are, for example, if statistics identify that crews were experiencing increased anti-social behaviour when visiting certain locations. The appliances that typically visit that area will only be affected and crews will be informed in advance. The audio capability of this equipment does not extend to routine monitoring within the appliance.

### 5.2 Responsible persons

**The Health Safety and Welfare (HSW) Manager** will have overall responsibilities for ensuring that the mobile CCTV and data recording system are used in accordance with all requirements within this policy, current data protection legislation and any other associated legislation. The HSW Manager will designate suitable staff, such as the HSW Practitioner/Officer for downloading any recorded data for reasons set out in this policy and will provide the necessary checks to ensure that the equipment and processes are being adhered to, which will be documented/logged.

**The Officer in Charge (OIC)** of the appliance and appliance drivers will ensure that the CCTV & data recorders are functioning in accordance with any Appliance and Equipment



(A&E) notes. Any faults must be reported to workshops by using the Trans 4 system. They will also ensure that camera lenses are kept free from dirt, debris and obstructions.

**The Workshops Manager** will be responsible arranging the installation and maintenance of the equipment in accordance with the manufacturer's instructions, the recording of specific vehicle performance data, and the coordinating of any maintenance requirements with an approved manufacturer/supplier.

**The Environmental & Energy Coordinator** will be responsible for gathering and reporting on environmental performance data only, such as vehicle emissions and fuel consumption.

These staff will only have the required permission to access the data they are concerned with and will use the appropriate information security measures relevant to that data.

**The Driver Trainers** will be responsible for viewing, downloading and utilising students' driving data and video footage for training purposes only. They will also ensure that the data used is deleted following training sessions.

### 5.3 Operational Guidance

All staff will follow guidance stated in Operational Guidance note (Appliance & Equipment Note) C01.01

### 5.4 Local Area Network (LAN) link

The mobile CCTV and data recording system has built in software that allows it to link in with the station Wi-Fi hub as soon as the vehicle returns to an AF&RS station. This will allow remote access to the data by authorised users. Data from the system will only be downloaded or viewed where there is a valid reason to do so in accordance with this policy.

### 5.5 Image storage, retention and deletion

Footage recorded on the vehicle's mounted hard drive will automatically overwrite as the hard drive reaches full capacity. This will depend on the size of the storage, the quality of the images and the frequency at which the devices are activated by vehicle movements. It is estimated that data will be stored for 30 days before it is overwritten which will give adequate time for it to be accessed when required.

The hard drive will be kept in a secure location on the appliance with restricted access and set permissions. Any footage viewed by authorised users will be transmitted via a secure server and any removable copies will be encrypted and/or password protected as per Service policies and procedures. Staff will also follow the Home Office guidance, [Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems guidance](#).





Data and video footage will only be downloaded and stored securely for the following reasons:

- A vehicle related accident, injury or near miss
- A report of violence or anti-social behaviour against AF&RS staff
- A receipt of a complaint about Service driving standards
- A formal request from an external agency in accordance with this policy
- A request from an individual to access personal information held (called a Subject Access Request (see Section 10 Requests of this policy)
- To monitor vehicle data such as engine emissions, fuel consumption or vehicle mileage
- To enable driver trainers to adequately provide feedback to driving students.

## 5.6 Training for operating the equipment

Authorised staff will be trained in accordance with the manufacturer's guidelines for operating the equipment. AF&RS will ensure that staff who operate the equipment for each of the various functional requirements and will be provided with the correct guidance material.

## 6 Fixed Installation CCTV

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 Location and positioning of the cameras

All of the AF&RS sites have fixed CCTV systems installed and will continuously capture images from cameras for up to 24 hours per day. The fixed cameras will be positioned to capture designated surveillance areas. For the avoidance of doubt these designated areas include;

- Perimeter boundaries
- Vehicle and pedestrian entrances & exits
- Fuel storage areas
- Vehicle appliance bay entry and exit
- High risk areas
- Control and IT equipment rooms

CCTV cameras will be positioned in such a way that they only monitor those spaces which are intended to be covered by the equipment and do not directly cover anyone else's property.



Cameras are to be located in full view of staff and the general public and are not to be used for covert surveillance purposes.

Cameras are positioned so that, where possible, they avoid capturing the images of persons not accessing our premises and any area outside of the perimeter of our sites

Clear CCTV signage must be placed to inform people that CCTV is in operation and these signs are openly visible to staff and the general public.

All proposed new installations of fixed CCTV systems including extensions and additions to existing systems must be approved by the Director of Legal & Corporate Services, whilst in consultation with the Property Services Manager and Control and Communications Group Manager.

## 6.2 Responsible Persons

- The Director Legal & Corporate Services** has overall responsibility for ensuring that all fixed CCTV systems are implemented and used in accordance with this policy and the AF&RS Physical Security Policy. The Director must approve the installation of all new installations and designate appropriately trained staff to use AF&RS fixed CCTV systems to view copy and download images and data.
- The Property Services Manager** is responsible for the installation and maintenance of all fixed CCTV systems. This includes agreeing the location of fixed cameras, installation of recording devices and CCTV viewing equipment, managing and responding to alert and alarm functions generated by the CCTV equipment, scheduled maintenance, repairs and replacement, and keeping an up to date Asset Register to include all CCTV equipment. The Property Services Manager will also maintain a list of staff (such as Security Staff) that have been designated by the Director of Legal & Corporate Services to view copy and download images and data from fixed CCTV systems within the requirements of this policy.
- The Control and Communications Group Manager (GM Control)** is responsible for the management of CCTV equipment located within our Service Control premises and access to CCTV images available for all other Service premises. They will ensure that all Control staff that are able to view fixed CCTV images do so in accordance with the requirements of this policy. The Station Manager (Control) will deputise in their absence. The GM (Control) and designated Control staff will only access the CCTV images in order to ensure effective operations for the Service, such as out of hours alarm activations on AF&RS premises and business continuity requirements (i.e. monitor bad weather conditions for appliance mobilisations). In addition, the GM Control will approve any image and data transfers across the AF&RS network to determine where fixed CCTV can be remotely viewed throughout our sites and provide advice on any potential disruptions to the network that may be caused through changes in the use of and installation of any new IT equipment, including CCTV.

## PREVENTING PROTECTING RESPONDING



- **Designated AF&RS Security, Health, Safety & Welfare, Property Services and other staff** who are able to view copy and download fixed CCTV images in order to conduct HSW investigations are responsible for carrying out these activities in accordance with the requirements of this policy.

### 6.3 Procedure

The following standards should be adhered to in order to ensure the effective operation of fixed CCTV systems.

- Following installation checks should be made to ensure cameras are working and correctly positioned.
- Camera positions and image capture should be reviewed at least annually by designated AF&RS security staff to ensure that it is still serving the purpose intended.
- All recording media and devices should be checked to ensure they are capturing images.
- If location, date and time information is recorded, these must be accurate and adjusted if required taking account of British Summer Time and other date adjustments.
- Cameras should be protected from damage and vandalism where possible.

### 6.4 Image storage, retention and deletion

All CCTV images are recorded locally. The retention of CCTV images is limited by the capacity of the recording media at each site, which ranges from 2 weeks to several months. Over time, images are deleted once the capacity of each device is reached. Images are not retained indefinitely within the fixed CCTV systems. Images can be downloaded for internal investigations, or when agreement has been made to release CCTV images to a third party (e.g. to an Enforcing Authority as part of a criminal investigation).

In the event that data is downloaded and retained as media evidence, it will be treated in accordance with the [Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems guidance](#), which is produced by the HM Home Office.

### 6.5 Training

Appropriate training will be provided in accordance with the current Information Commissioners CCTV code of Practice and the Home Offices Surveillance Camera Code of Practice 2013.

The Property Services Manager (or designated person) will arrange for introductory or familiarisation training, in the use of the system, to all staff required operating the CCTV system.



The Director of Legal & Corporate Services will nominate and agree which staff will be permitted to access and/or operate the CCTV system.

Operators will receive training and will be required to familiarise themselves with the following:

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

## 6.6 Maintenance

All cameras, associated ancillaries, recording equipment / media and viewing devices require a scheduled maintenance and servicing programme by an approved contractor. This must include a call out service in the event that any part of the system fails or is damaged.

The operators of CCTV equipment will check the equipment on a weekly basis to ensure performance and reliability by the viewing of live and recorded imagery. The Property Services department will be informed of any failure/ malfunction/ unsatisfactory performance and will instruct the approved maintenance contractor to attend and rectify all failures.

**A servicing and maintenance record of all CCTV must be maintained by the Property Services department to include scheduled maintenance and all system failures and call outs.**



## 7 General Signage

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

All AF&RS buildings/premises, locations and vehicles where CCTV systems are in use will prominently display public awareness signs detailing:

- That CCTV cameras are in operation
- Where possible, Service contact details if a member of the public has any concerns or would like to make a request for information
- Signage showing a picture of a camera
- Where possible, the purpose of CCTV system

## 8 Data Security

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. AF&RS is registered as a 'data controller' with the Information Commissioners Office. As part of our 'privacy notice' (or sometimes referred to as a 'fair processing statement') the Service will specify what types of personal data we process and the reasons why. We must therefore ensure that the purposes for collecting and processing CCTV and associated electronic recordings, remains up to date.

Data obtained from the various CCTV equipment must only be accessed, downloaded and stored by designated staff on AF&RS owned equipment, with suitable access controls and security measures set.

Any equipment used in connection with the access of data from stored images will adhere to the Service's policies, and will be suitably encrypted/password protected whilst in use and will be erased or destroyed once the purpose of the recording is no longer relevant.

Recorded media no longer in use will be securely destroyed by approved contractors who will issue a destruction certificate for our records.

All equipment will be logged by AF&RS for asset records management.

In the event that equipment that contains personal data needs to be accessed by a contractor for maintenance issues, AF&RS will request that the contractor signs a Non-Disclosure form. This is to ensure that any personal data that the contractor has access to is not inappropriately processed.

Any information captured by the CCTV and associated equipment will be handled as per this policy. In the event of any inappropriate use of data or the Service's CCTV equipment that contradicts this policy or any other policy or procedure, such as the AF&RS IT

**PREVENTING PROTECTING RESPONDING**





Acceptable Use Policy and the Social Media Policy, may result in an investigation which could potentially lead to disciplinary action.

In the event that any CCTV equipment or associated data is lost, stolen or inappropriately used, staff need to report this as a 'Data Security Breach' via Service Control, so appropriate action or advice can be given and the incident logged onto the Service's Health, Safety and Welfare system and suitably investigated.

## 9 Requesting copies of CCTV images, audio and data

Data Protection legislation, (The Data Protection Act (DPA) 2018 and the EU General Data Protection Regulations (GDPR) 2016) is a framework of rights and duties which are designed to safeguard personal information. AF&RS has a duty of care to ensure that all personal information is handled responsibly and in a fair legal way. Details of our [Privacy Notice](#), and [relevant policies](#), including what we do with personal information can be located on our website.

Under data protection legislation an individual (the data subject who is the applicant) can submit a Subject Access Request (SAR) and, providing it is a reasonable request, AF&RS are obliged to comply. Individuals have a right to view any personal information that is held about them by an organisation. This provides them with the opportunity to ensure that the personal information that AF&RS holds is correct.

Personal information can be held in various forms, such as electronic, paper and, also visual images and audio, where a living individual can be identified from that information or together with other information that is or may come into the possession of AF&RS.

SARs within AF&RS are coordinated and processed by the Data Protection team and are dealt with on a 'case by case' basis. AF&RS do not charge for processing SARs and will retain correspondence for three years in accordance with SAR Retention Schedule.

Please visit the [Data Protection Act page](#) on our website to find out more about the Act and if you wish to submit a request under current data protection legislation in relation to personal information that we hold about you. Individuals may wish to use the '[Contact Us](#)' page of the website, alternatively you can write to us:

Data Protection Team  
Avon Fire & Rescue Service  
Police & Fire Headquarters  
PO Box 37  
Valley Road Portishead  
Bristol BS20 8JJ

**Email:** [FOI-DP@avonfire.gov.uk](mailto:FOI-DP@avonfire.gov.uk) **Telephone:** 0117 926 2061 - Headquarters switchboard

**PREVENTING PROTECTING RESPONDING**

Version: 1	Next review: 03/01/2019	Closed Circuit Television (CCTV), Video and Audio
Status: Awaiting Review	Issue date: 03/01/2018	Recording Equipment and Vehicle Data Devices





Avon Fire Authority (operationally known as Avon Fire & Rescue Service) is defined as a 'Data Controller' for the processing of personal data within the Service. All staff, Members, Contractors, and Volunteers have a responsibility for data protection.

All information processed in relation to this Policy will be in accordance with our Data Protection and Information Security Policies, and our Privacy Notice, which are freely available on our website at [www.avonfire.gov.uk/guide-to-published-information](http://www.avonfire.gov.uk/guide-to-published-information), and [www.avonfire.gov.uk/privacy](http://www.avonfire.gov.uk/privacy), and any suspected data breach of personal or sensitive data will be reported without delay.

We have a number of statutory responsibilities, powers and duties which require us to carry out certain tasks, and we collect and use only the personal information necessary to meet these purposes. We will always ensure your data is treated fairly, transparently, and securely.

Further information is available from the AF&RS Data Protection team, or from the Information Commissioner's Office website at [www.ico.org.uk](http://www.ico.org.uk).

## 9.1 Freedom of Information Act

Under the Freedom of Information Act 2000 (FOIA) individuals have the right to request recorded information that AF&RS holds. Such requests are coordinated by the Data Protection Team. and must be responded to within 20 working days of receipt of the request (subject to any clarification). Each request for recorded images/audio made under the FOIA will be considered on an individual basis.

Like all legislation there are exemptions. Section 12 of the FOIA allows a public authority to refuse a request where it is estimated that it would exceed the appropriate cost limit of £450, which equates to 18 hours of work to determine whether the information is held, locating, retrieving, and extracting it into a suitable format that the information can be provided to the applicant. Where this is apparent, AF&RS will advise the applicant and provide advice to help the applicant refine the request so it can be dealt with within the appropriate limit.

AF&RS will retain any request correspondence for the current financial year, plus three years in accordance with our Retention Schedule.

### Personal Information

Section 40 'Personal Information' of the FOIA exempts information about individuals from being disclosed. If the images or audio in question are that of the applicant, then the request will be dealt with as a Subject Access Request under the data protection legislation, as above.

## PREVENTING PROTECTING RESPONDING

Version: 1	Next review: 03/01/2019	Closed Circuit Television (CCTV), Video and Audio
Status: Awaiting Review	Issue date: 03/01/2018	Recording Equipment and Vehicle Data Devices



### Images of other people:

Where a request is made from a third party, for footage that includes identifiable images of other individuals (the data subjects), this is classed as personal information about the individuals concerned. It is unlikely that such information can be disclosed in response to an FOIA request as the applicant (third party) could potentially use the images for any purpose and the individuals concerned are unlikely to expect this. This may constitute as unfair processing in breach of the data protection legislation.

### Audio recording of other people

The same principle as above applies to audio recordings that are requested by third parties (not the individual(s) voices that are captured by that recording), if those individuals can be either identified by that recording or that recording together with any other information that comes into the possession of the applicant.

However, in some circumstances it may be lawful to provide details of the recording without breaching the data protection legislation, such as providing the applicant with redacted scripts (subject to exemptions, such as the cost limits). The reason for the request will be taken into account, each request will be considered on an individual basis and legal advice maybe sought.

## 9.2 Requests from agencies and other organisations

We may receive requests for evidence from other agencies and parties such as the Police, insurance companies and legal organisations, and these will be dealt with under terms of the Freedom of Information Act 2000. We would still need to consider if any personal information we release is subject to the data protection legislation and this will be dealt with appropriately. When supplying any information to the Police, we would require the appropriate signed data release forms and will provide any information via a secure method. Please direct any enquiries via the contact details above.

Should members of AF&RS staff receive any external requests for copies of CCTV footage, please direct any such requests to [FOI-DP@avonfire.gov.uk](mailto:FOI-DP@avonfire.gov.uk) or the member of the public can complete an online form on the AF&RS website <http://www.avonfire.gov.uk/guide-to-published-information/freedom-of-information>. Requests need to be in writing and AF&RS will consider every request on an individual basis.



### 9.3 Internal AF&RS staff requests for copies of CCTV/audio data

This part of the policy applies to members of AF&RS staff who are **not Service approved designated users** of the various CCTV equipment.

Should a member of staff require access to footage or any other data captured by the various CCTV footage, please follow the below guidelines:

- If the member of staff is seeking personal information about themselves that is captured by any of the CCTV equipment, audio and related data, this will be processed as a **Subject Access Request** (as above). Staff can also seek guidance from the Data Protection pages of the internal staff intranet or discuss their requirements with the Data Protection Team. Any such requests need to be in writing or via email.
- AF&RS will not allow access to CCTV footage to any member of staff without prior written authorisation from a member of SMB (for which they must have a valid business reason).
- Health, Safety and Welfare incidents involving AF&RS staff, premises, vehicles and visitors to our sites should be reported via the Services Wellworker (OSHENS) process so it can be appropriately investigated. As part of the investigation process, a decision will be made regarding the sharing of the footage. For AF&RS staff working as an Investigating Officer for a wellworker (OSHENS) incident, then authorisation can be provided by the HSW Manager.

### 9.4 Other requests regarding the processing of personal data

In addition to the right of access to their own personal data (SAR), individuals have other rights under data protection legislation, such as the right to (please note this is not an exhaustive list):

- be informed when processing is taking place;
- prevent the processing of personal data in certain circumstances ; and
- correct, rectify, block or erase information that is regarded as 'wrong information' if it causes, or is likely to cause them substantial and unwarranted distress and harm.

Any requests regarding an individual's rights under the data protection legislation , must be passed to the Data Protection Officer who will ensure that a decision is made as to 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

## PREVENTING PROTECTING RESPONDING



response to the individual. A copy of the request, response and any decision information will be retained for our records.

---

## 10 Appeals and Complaints

AF&RS are committed to providing a professional and efficient service. However, if you are unhappy with the way your request for information has been handled, you can request an internal review by writing to the

Clerk to the Fire Authority  
Avon Fire & Rescue Service  
Police & Fire Headquarters  
PO Box 37  
Valley Road Portishead  
Bristol BS20 8JJ

Telephone 0117 9262061 or by emailing [FOI-DP@avonfire.gov.uk](mailto:FOI-DP@avonfire.gov.uk).

If you remain dissatisfied with the handling of your request for information, you have the right of appeal to the Information Commissioner at:

The Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Telephone 0303 123 1113 (local rate) or 01625 545 745. Website [www.ico.org.uk](http://www.ico.org.uk)  
There is no charge for making an appeal.

For non- personal information related enquires, and as part of our commitment to provide a good service, we also operate a complaints process. Should you need to make a complaint, you can either submit your complaint via our website page <https://www.avonfire.gov.uk/contact-us/non-emergency/how-we-handle-comments-compliments-and-complaints>, or you can write to us FAO: Corporate Performance Manager at the AF&RS Headquarter address. A copy of our Complaints Policy is also available via our website or we can provide you a copy on request.


**Document Control Information:**

<b>Policy title:</b>	Closed Circuit Television (CCTV), Video and Audio Recording Equipment and Vehicle Data Devices
<b>Policy owner: (role)</b>	Area Manager, Operations Response
<b>Author: (role)</b>	Health & Safety Advisor
<b>Authoriser: (role)</b>	ACFO / Service Delivery
<b>Issue status:</b>	Awaiting Review
<b>Protective marking:</b>	-
<b>Issue date:</b>	03/01/2018
<b>Next review due:</b>	03/01/2019
<b>Audience:</b>	For external publication
<b>Version Number:</b>	1

**Equalities Impact Assessment (EIA) Information:**

(EIAs should be reviewed and updated alongside the policy)

<b>EIA Required: (Yes/No*)</b>	Yes - completed
*If No, an EIA template <b>must</b> be completed up to and including Part 4 (the 'opt out' section).	

**PREVENTING PROTECTING RESPONDING**

Version: 1	Next review: 03/01/2019	Closed Circuit Television (CCTV), Video and Audio
Status: Awaiting Review	Issue date: 03/01/2018	Recording Equipment and Vehicle Data Devices

Uncontrolled when printed – check on line to check latest version



**Document History:**

Review Date	Version No	Summary of Changes	Equality Impact Assessed (Y/N)
12/07/2019		Data Protection information updated	

**Distribution History:**

Date	Version No	Distributed to: (role/s or group/s)
10/08/2017	0.1	Informal consultation to Unit Heads and Rep Bodies
03/01/2018	1.0	Publication

**PREVENTING PROTECTING RESPONDING**

Version: 1      Next review: 03/01/2019      Closed Circuit Television (CCTV), Video and Audio  
 Status: Awaiting Review      Issue date: 03/01/2018      Recording Equipment and Vehicle Data Devices