SERVICE INFORMATION SYSTEM	
Title	**Digital Imagery**
Category	**Operations**
Number	**B28**
Status	**v3.0**
Action	**All Northamptonshire Fire and Rescue Service (NFRS) personnel**
Original author	**Area Manager – Corporate Services**
Protective marking	**Official**
Executive summary	This policy gives guidance to all personnel on the capture, process and storage of digital imagery. Employees should also refer to service policy A45 – Social Media.

Contents

Job title	**Area Manager – Business Services**
Date	**October 2016**
Review due	**October 2018**

1 INTRODUCTION

This policy gives guidance to all personnel on the capture, process and storage of digital imagery.

The following relevant NFRS policies and Standard Operating Procedures (SOPs) should be read for specific information/procedures:

- Service policy A45 – Social Media
- Service policy B1.3 – Command Development Centre (CDC) (Fire Control Room/Incident Room) Ambient Recording
- Service policy B7.1 – Fire Appliance Mounted Closed Circuit Television (CCTV) Camera
- SOP F6 – Body Worn Video (BWV)
- SOP F12 – Evidence Gathering – Digital Photography
- SOP F15 – Investigation and Evidence Gathering Procedures

2 LEGISLATION AND NFRS COMPLIANCE

The following Legislation and legislative guidance is complied with by NFRS:

- Article 8 of the European Charter of Human Rights
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act (RIPA) 2000
- Information Commissioner's Office (ICO) Data Protection, CCTV Code of Practice (current version)
- Home Office: Surveillance Camera Code of Practice
- Home Office guidelines, "Guidance for the police use of body-worn video devices"
- Section 30 (1) (a) of the Protection of Freedoms Act 2012
- Copyright Act (image age dependant; see below)

The above legislation and guidance does stipulate specific elements which apply to data storage, consent and deletion of data; NFRS application of said elements is detailed in the specific sections to which it applies below or in the policies referenced in section 1 – Introduction.

Images obtained at incidents are for Fire Service use only or, where legislation requires, for shared use by other Emergency Services and Security Services for investigative purposes.

Publication of images identifying individuals or property without some form of consent of the subject or property owner or without making the image anonymous may be considered a breach of legislation and could lead to legal action against the Fire and Rescue Authority and subsequent adverse publicity.

It is vital that employees understand that imagery obtained at commercial premises have been granted under the Fire and Rescue Services Act 2004, in connection with gathering risk information. Disclosure of such imagery would be likely to constitute a breach of the confidential nature of the information provided to the Service and this could have serious legal repercussions.

3 IMAGES TAKEN BY EMPLOYEES ON DUTY

A manager may authorise the capture of images for operational, intelligence, training or debrief purposes. The authorisation to obtain imagery should only be given for the following reasons:

- To enhance risk information about a premises or a location.
- To assist with the debrief of an incident or to illustrate learning points from an incident, exercise or training event.
- As part of the evidence gathering process where a criminal offence may have been committed or legal action seems likely following an event.
- For Safety Event Recording. Refer to service policy E2 - Safety Event Reporting and Investigation Procedures.

3.1 Images as evidence

Fire Investigation Officers (FIOs) and Fire Protection Officers (FPOs) may obtain any images that they deem necessary to assist their investigation. Whilst the audit trail for the images must be strictly adhered to, it is not the intention of this policy or the procedures to constrain and prevent them from lawfully obtaining evidence.

Any images captured by FIOs and/or FPOs whilst undertaking their duties will be retained by the FIO/FPO and the following procedures must be adhered to:

- Service Policy B7.1 – Fire Appliance Mounted Closed Circuit Television (CCTV) Camera
- SOP F6 – Body Worn Video (BWV)
- SOP F12 – Evidence Gathering – Digital Photography
- SOP F15 – Investigation and Evidence Gathering Procedures

Images/imaging captured by Appliance Mounted CCTV or Unmanned Aerial Vehicle (UAV)/Unmanned Aerial System (UAS)/Drone are managed by Joint Operations Team (JOT) in line with the above policies and procedures.

3.2 Taking images at the Incident Ground

Images will only be taken when:

- It is safe to do so
- Permission from the Incident Commander (IC) has been given
- It does not compromise operations in progress or scene safety

The use of cameras to obtain images as potential evidence will only be authorised by a manager under the circumstances listed below:

- Incidents where the Police are not in attendance and it is suspected a crime may have taken place and it would be detrimental to the evidence to await their arrival before images are taken.
- No Scenes of Crime Officer or FIO is in attendance and images need to be recorded for fire investigation purposes.
- It is suspected that there is a breach of fire precautions legislation and this must be recorded without delay otherwise the evidence may be lost or interfered with.
- In the case of fire investigations or other potential crime scenes, it will often be sufficient for images to be obtained of the outside of a premise, as Fire

and Rescue Service personnel will have difficulty in controlling such areas before the arrival of the Police.
- Images should normally only be obtained from inside the premises in instances where the evidence is likely to be lost due to progression of an incident, weather conditions, the potential for removal or tampering by third parties or due to things being moved or cut away for rescue purposes.
- To document safety event information as per service policy E2 - Safety Event Reporting and Investigation Procedures.

The balance between capturing vital imagery for evidence and unnecessarily entering a potential crime scene and possibly introducing contamination or destroying evidence is one that can only be made by the manager at the incident. However, it should be thought through fully before authorisation is given.

All imagery obtained by NFRS employees at the Incident Ground in general operational circumstances (non-crime scene) must be forwarded to the JOT. They will, in liaison with the Northamptonshire Police News and Publishing Team, classify captured images and upload as appropriate to the relevant area on FirePlace (see section 8).

3.3 Taking Images to Aid Risk Information Sharing

NFRS personnel required to take digital images for the enhancement of risk information PowerPoint presentations, will be required to get permission from the owner/occupier site representative prior to taking any images.

Consent must be obtained by completing the FB161b consent form, on the initial visit, if the owner/occupier site representative is not available to do so at the time, no images may be used until consent has been granted. The completed consent form must be submitted to the Risk Intelligence Technician (RIT) with all other documentation when completing a Site Specific Risk Information (SSRI) visit. If a use of digital imagery request is made after the completion of an SSRI the FB161b should be forwarded to the RIT and added to the file.

All captured images to be used in presentations must be uploaded to the Operational Library on the Digital Imagery site on FirePlace. Images that are not used for this purpose must be deleted.

Images containing certain details will need sanitising prior to use in presentations and the following section offers clarification of the requirements when taking images:

- You must have consent from the owner/occupier site representative to take images of the premises
- All identifiable features should be avoided when taking pictures or MUST be removed from the image, these include registration plates, street names and people
- The image should be of a good quality
- The image should be relevant to your area of work

Images used for the purpose of these presentations must only be stored in the central area. No images will be duplicated and held elsewhere other than within the presentations.

4 TAKING IMAGES AT A PUBLIC EVENT OR IN A PUBLIC PLACE

There are no laws specific to the act of taking photographs in a public place, it is the intended use that is subject to principles of the Data Protection Act 1998.

Taking a photograph of a person does not require written consent so long as it is taken in a public space where the person did not have a reasonable expectation of privacy and where an identifiable person is not the subject of the image. Therefore, if images are taken at a public event attended by large crowds, such as a fire station open day, permission to capture digital images is not needed of everyone in a crowd shot.

People in the foreground are also considered to be in the public area, however, photographers must address those within earshot, stating where the photograph may be published and giving them an opportunity to move away.

4.1 Identifiable Images taken at a public event

If you choose to take any shots of a small number (up to five) of people at any event or in any public place **where an individual is clearly identifiable**, for example in a close up shot, you should expressly ask for their permission and let them know of the intended use for the photographs to comply with data protection principles.

This gives people the option to opt out and will help to avoid any misunderstanding leading to harmful consequences for the photographed individual(s) and legal claims against the Service for breach of the Data Protection Act 1998.

Adults

Consent can be gained verbally in this instance. If you wish to take people's names or any other personal information to use in a caption to accompany the identifiable image or footage, you must ensure that your intentions are clear when asking for this additional personal information. Also refer to section 5 – Posed Photographs consent.

Children and young people (under 18 years of age)

Where the image is of identifiable children and young people (under 18 years), you must ask for written consent using FB161 form. The consent form must at all times be stored with its related image. Also refer to section 5 – Posed Photographs Consent.

4.2 Further precautions

Further precautions to allow people to opt out or avoid the area being photographed or filmed:

- When sending out invitations or advertising an event it is considered best practice to specify that a photographer will be taking photographs during the event.
- Signs should be placed in a prominent place and at entry points to inform people that the event will be photographed or filmed.
- Ensure that the photographer or person filming is clearly identifiable so people can stay out of any area being photographed if they so wish.

4.3 School events organised in liaison with educational establishments

Personnel organising events in liaison with educational establishments i.e. school, nursery etc. must obtain photo/video consents for children involved in the event.

The consents should be available on request from the educational establishment and should be requested in the planning stages of the event to avoid delays in publication of digital content created during the event.

5 POSED PHOTOGRAPHS CONSENT

A person's consent is needed (or parental consent for those under 18) to publish photographs when they are clearly recognisable in a posed image.

This is particularly important when dealing with children, and permission must be obtained from the parent or guardian of any child or young person up to the age of 18. This is not applicable for images captured on appliance CCTV systems or premise CCTV systems.

If two parents disagree over consent for their child to appear in images, consent has not been given. If the parents agree to consent, but the child does not, consent has not been given.

Before taking any images of people (data subjects), it must be made clear to the data subject:

- Why their image is being used
- What the image will be used for
- Who might look at the image

Their consent **must** be obtained, using consent form FB161 or FB161a Responsibility for obtaining the consent lies with the person(s) organising the image capturing. Therefore the data subject(s) should fill in or agree to fill in the forms prior to any department arranging for any form of image capturing.

Consent forms, once completed, will be uploaded with their related images to the appropriate area on FirePlace and a link to the consent form should be held within the metadata of the relevant image (see section 8).

5.1 Agency images

If photographs are obtained from an agency, the agency must guarantee in writing that permission has been granted. Wherever possible, images that portray Northamptonshire people and Northamptonshire sites should be used.

The agency needs to be informed how the photographs will be used. Ultimately however, it is the responsibility of the Service to ensure that the agency has obtained permission from the people in the photographs.

5.2 Employee images

Photographs may be taken of NFRS employees in the line of duty or during training exercises and in these circumstances the images become the property of NFRS. However, respect for their privacy should be considered according to Article 8 of the European Convention of Human Rights. Where an employee is

easily recognisable, permission to publish images outside the workplace must be sought using form FB161a or written into contract of employment.

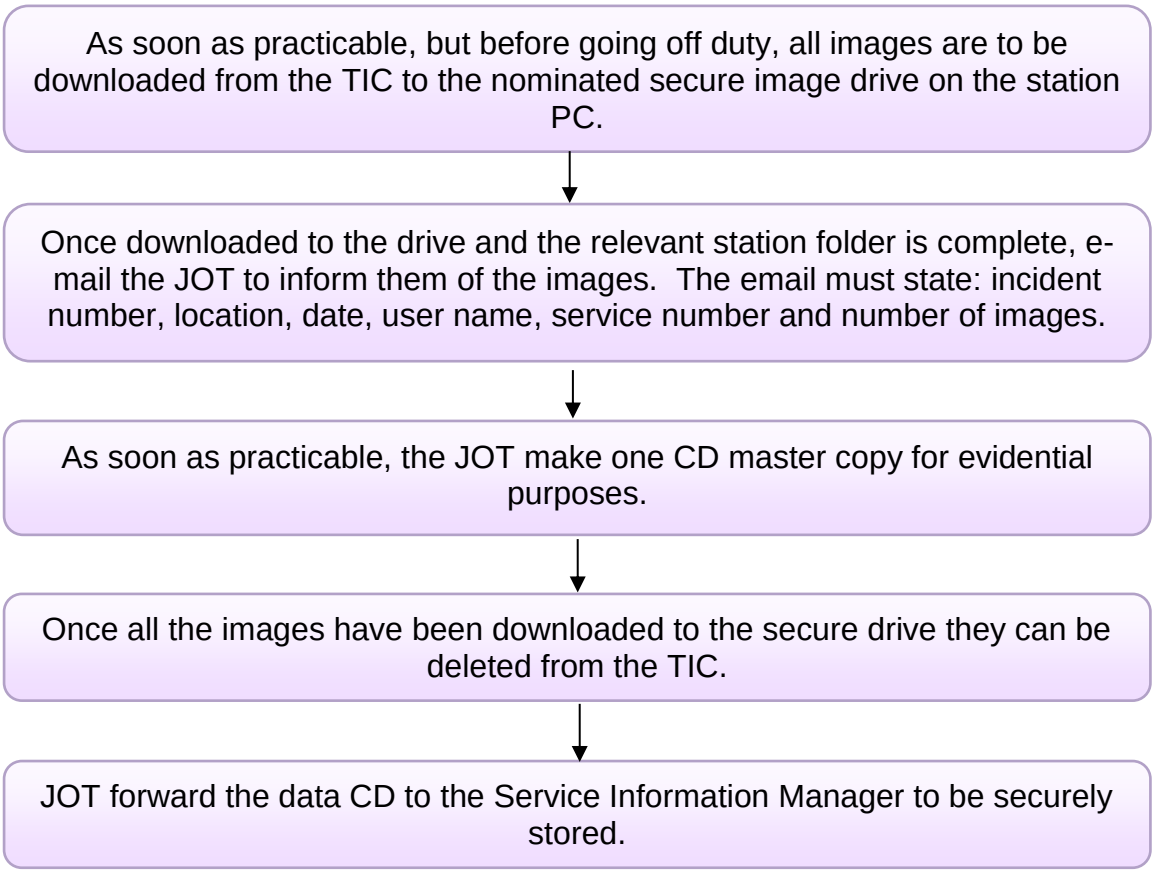
Alternatively the images must be made anonymous. Images are personal data and individuals must have their wishes respected.

6 SECURITY PHOTOGRAPHS

An image taken for security reasons, e.g. to enable access to a buildings, is a legitimate business purpose for processing personal data. However, unless the employee agrees, these images cannot be used for any other purpose.

7 THERMAL IMAGE CAMERA (TIC) – IMAGE CAPTURE AND STORAGE

Following is the process flowchart for all occasions the TIC is used to capture an image:



8 PROCEDURE FOR STORAGE OF IMAGES

Prior to classification, captured images should initially be stored on NFRS secure drives only and not kept on portable drives, personal drives or private storage areas.

Once classified, all images are to be stored on FirePlace > Service Information System > Digital Images Store.

The Digital Images Store site will allow access to sub sites which hold libraries of similarly categorised images.

Security is applied to each library on an individual basis. If a user has no access to a library then that library will not be visible to them.

One image or many can be uploaded to the relevant library at a time. Mandatory metadata will need to be applied to uploaded images.

The metadata required is set on a per library basis but will include:

- Date image taken
- Image expiry date
- Location or address
- Brief description
- Incident number or other unique reference number (if applicable)
- Who took the images
- Who uploaded the images
- A link to related consent form FB161/FB161a/FB161b (if applicable)

A nominated person within individual departments will be responsible for creating image libraries as required, setting the required metadata and uploading images.

Where digital images are intended for publication and circulation within and outside the Service they must either:

- Be linked to a signed consent form within metadata, or
- First have been sanitised and made anonymous (sanitisation could include masking the identification of individuals or items, including vehicle registration numbers, house names etc.)

Images which require sanitisation prior to publication must be forwarded to the Northamptonshire Police News and Publishing Team along with instruction. Once this process is complete the Service Information Team will upload the images as per instruction.

The nominated person within individual departments will be responsible for ensuring that images are destroyed once consent has expired, which will normally be 2 years from the date of the consent form, unless otherwise agreed and stipulated on the consent form.

Photographs or images of service personnel will normally be retained for the duration of an employee's service, unless advice is given otherwise.

9 COPYRIGHT

It is important to be sure of the copyright position of any photographs you intend to use; under the laws of copyright photographic images are considered as artistic works.

Copyright is basically the right given to authors and creators of works to control the exploitation of their works. This right broadly covers copying, adapting, issuing copies to the public, performing in public and broadcasting the material.

Copyright arises automatically and does not depend on the completion of any formalities, such as registration. Remember that photographs obtained from the Internet are also subject to copyright. The first owner of copyright is usually the author of the work.

The major exception is where such work is made in the course of employment, in which case the employer owns the copyright.

Commissioning and paying for work does not procure the copyright.

Contractors and freelancers own the first copyright in their work unless the commissioning contract agrees otherwise. You should also remember that copyright lasts for over 50 years. Photographs taken after 1 August 1989 are protected for 70 years after the death of the photographer.

There are different rules regarding older photographs depending on the relevant Copyright Act at the time they were taken.

More information on copyright is available from the United Kingdom's Copyright Licensing Agency www.cla.co.uk or International Federation of Reproduction Rights Organisation in Brussels www.ifrro.org.

10 MISCONDUCT

On duty employees of NFRS obtain images not as an individual, but as representatives of the Service. Every act carried out whilst on duty (and also inappropriate acts or actions carried out whilst off duty) would reflect upon the Service.

It must be clear to all concerned that there are associated risks as well as benefits for the Service in allowing employees to obtain images. For this reason, and in order to safeguard people's human rights, control measures need to be put in place.

The use by employees of any device which captures images must be authorised by an IC at an incident, or a Station Manager (SM) or equivalent on all other occasions. The procedures detailed in this policy document are to be adhered to by all personnel.

All images obtained by employees whilst on duty remain the property of NFRS and may not be used or viewed by third parties or posted to social media sites without permission of a Principal Officer or as detailed in specific procedures e.g. photographs for investigations are detailed in SOP F15 – Investigation and Evidence Gathering Procedures.

Confidential, internal-use only or copyrighted images that belong to NFRS or third parties must not be posted to social media sites or otherwise online prior to classification and without written permission. For further guidance refer to policy A45 – Social Media.

The misuse of imaging equipment by employees, including but not limited to cameras, printers, copying facilities, other associated equipment or software, including the images themselves, is regarded as a serious matter which may result in disciplinary action, including dismissal from the Service as per service policy A23 – Disciplinary Procedure.

11 PERFORMANCE AND REVIEW

This policy document and its associated procedures are consistent with national digital imaging legislation and guidelines and will be reviewed every 2 years.

This will not negate the need for review and amendment following changes in legislation, procedures and national guidance.

Specific audits may be undertaken of any part of the process at the discretion of the Service Information Manager.

12 CLICK TO CONFIRM UNDERSTANDING OF THIS POLICY

All personnel are required to click the button below to go through to RedKite to confirm that you have read and understood this policy:

Click to Confirm Understanding

Document Control			
Version	**Date**	**Author**	**Status**
1.1	June 16	SIT	Draft
1.2	August	SIT	Draft
2.0	06/10/16	SIT	Published post approval at TLT meeting