East Midlands

Protective Marking: **OFFICIAL**
ID Code: POL-B28-v1.0
Author: Joint Operations Team
Published: 27/01/2023

Policy Note
Operational Digital Data

Introduction
This Policy details how Northamptonshire Fire and Rescue Service (NFRS) manages digital data in the operational environment. The service position on data protection, Imagery and CCTV will be dealt with in separate documents

Contents

1. Policy Statement

1.1 Operational Digital Data covers

- Images captured in the operational environment including on station and station events.
- Ambient Recording in Fire Control and the Joint Command Unit.
- Thermal Image Cameras.
- Body Worn Cameras/mobile devices
- Incident Data (Command support packs)

1.1.1 Capturing Images and Video

- Images or video captured on a mobile device in a work setting must be treated responsibly. While it is permitted to take pictures in the public environment, as it would be if you were a member of the public, there are certain times when taking a photo without permission would not be permitted:
  - Taking pictures of children.
  - Taking pictures of individuals where there is a reasonable expectation of privacy.
  - Taking pictures without permission on a premises of a site not owned by you such as a commercial property.
  - Taking pictures of a crime scene (unless authorised by your manager).
  - Taking pictures that may affect an individual's right to privacy such as through windows of private property.

1.1.2 Management of images and video

- Images or video captured for private use must remain private and not shared unless:
  - Publishing them on social media complies with the Social Media policy.
  - They are to be used as evidence.
    - In this instance the images should be submitted to the body requesting the evidence then deleted from the device.
  - They are used for training.
    - Images captured should be sent to media and comms for storage on the service secure data storage system (digital images store)
  - They are used for risk intelligence.
    - Permission must be granted for use and the images should be stored securely.
  - They are used for Operational learning.
  - They are used for promoting the service. This should be done in conjunction with the media and communications department.

1.1.3 **Retention of images and video**

- All images and video captured and stored on service systems will be stored in accordance with the service retention schedule.

1.1.4 **Ambient recording**

- Ambient recording is the facility of capturing audio/visual activity within a room at the touch of a button. Currently this facility is available in Fire Control and on the Joint Command Unit. A separate operational information note details the operational use. Data will be stored on secure drives in accordance with the service retention schedule.
- To let everyone, know that recording is taking place a red light stating “Recording” will illuminate when the system is activated.

1.1.5 **Thermal Image Camera (TIC)**

- Images from thermal image cameras should be downloaded as soon as possible to the computers on stations. The station will inform JOT (Joint Operations Team) who will make a copy onto a disc and then transfer the images to the digital image store on Fireplace. The imagery on the camera must then be deleted.

1.1.6 **Appliance mounted CCTV**

- This area is covered in a separate policy statement Policy B7 Fire Appliance Mounted Closed Circuit Television (CCTV) Camera

1.1.7 **Body Worn Cameras**

- Northamptonshire Fire and Rescue Service own and/or operate systems intended to overtly capture video and voice data during their duty, such as operational incidents, exercises, and other appropriate operational training events.
- Body Worn Video (BWV) is the term used to cover the video capture that is mobile and positioned on an operator or on a suitable apparatus. It may also be used in a similar manner to that of a handheld video camera.
- It cannot be ruled out that third parties (e.g., members of the public) may be captured during any recording. To comply with our responsibilities under the Data Protection Act all staff will receive appropriate training and a procedural document detailing how/when the devices can be used will be maintained.

1.1.8 **Operational Documentation**

- All Operational Data collected at incidents will be stored on secure drives and will be retained in accordance with the service retention schedule.

1.1.9 **Responsible persons**

- The following posts have responsibility under this policy statement

  - **Service Data Protection Officer (DPO) -** Responsible for advising on compliance with Data Protection Act 2018 and Freedom of Information Act 2000 and BAU related to these Acts
  - **Digital & Technology Lead Response –** Responsible for ensuring IT infrastructure in place to manage the requirements of the Service delivery and the information compliance
  - **Joint Operations Manager –** Responsible for the maintenance of this policy and procedural documents
  - **NFRS Staff –** Responsible for day-to-day operation of the systems and ensuring compliance with Data Protection Act procedures detailed in this policy

This Version No.		1.0	
Replaces		N/A	
Summary of changes		N/A	
Versions	**Date**	**Modified by**	**Changes**
1.0	27/01/2023	Joint Operations Team	New policy
Department		Joint Operations Team	
Assessments completed		EqIA	
Date Published		27/01/2023	

Derbyshire☐ Leicestershire☐ Lincolnshire☐ Northamptonshire☑ Nottinghamshire☐