	UNIFIED FIRE AUTHORITY **ORGANIZATIONAL POLICY MANUAL**	
	Affiliation: Administration Policies	
	Title: **Management of Photos, Recordings, and Other Electronic Media** Number: **100 – 310**	
	Approved: 6/9/2021	By: Fire Chief Dan Petersen
	Last Reviewed: 12/10/2025	By: AC Wade Russell

REFERENCES:
Utah Government Records Access and Management Act UCA§63G-2-101 ("GRAMA")
Public Records Management Act UCA§63A-12-100
UFA Policy and Procedure – Patient Request to Access Protected Health Information (PHI)

DEFINITIONS:
UFA Owned Media: Photographs, digital photographs, digital images, video recordings, electronic files containing an image or series of images, or any audio recordings as well as any digital reproductions or copies of such photographs, digital photographs, digital images, video recordings, audio recordings, or files, owned by UFA because they were taken and/or created while on duty and in the course of UFA's business, regardless of whether taken or recorded on UFA-Owned or personal imaging or recording devices. This definition expressly includes the live streaming of imagery whether recorded at the time of creation or not. This definition may also be referred to in this policy as department owned images, department owned digital images, or department digital images.

Imaging device*:* Any device capable of producing a digital image (including but not limited to a cellphone, smartphone, tablet, iPad, computer, drone, digital camera, or digital camcorder) or analog image, including photographs or film recordings.

Recording device*:* Any device capable or recording audio, whether digital or analog.

PURPOSE:
The purpose of this policy is to provide guidance on the creation, collection, and maintenance of photographs, recordings, video, and other electronic media created by or on UFA equipment or by personnel on personal equipment while on duty in order to comply with the law, maintain the professional image of UFA, and protect the privacy rights of UFA personnel, patients, fire victims, and the public.

POLICY:
The proper functioning of any fire and emergency service organization depends upon the public's confidence and trust in the individual firefighters, officers, and department to carry out our mission. Any conduct that brings discredit to individual firefighters, officers, or UFA has the corresponding effect of reducing public confidence and trust in our organization, thus impeding our ability to work with and serve the public. Professionalism is a significant factor in high level performance which in turn builds the public's confidence and trust.

In addition, when the public calls upon the UFA for help they have a right to expect that we will keep the details of their private lives and affairs confidential, and not release that information, except as permitted by law. When the public lacks confidence in our ability to provide our services, they may delay reporting emergencies or refuse to report emergencies resulting in unnecessary death and destruction, thereby causing actual harm and/or disruption to our mission and function.

It is the policy of UFA to respect the privacy interests of department personnel, patients, fire victims, and the public, and to comply with the state laws related to public records. It is further the policy of UFA to respect and protect the medical confidentiality rights of department personnel, patients, fire victims, and the public as required by federal and state law.

1.0 IMAGING AND RECORDING IN GENERAL

Subject to the prohibitions and exceptions provided for in this Policy, UFA employees are strongly discouraged from using a camera, video recorder, audio recorder, a camera/video/audio function of a cellular phone, or any other digital imaging device or recording device, to capture digital media while on-duty. The Fire Chief may grant an exception to this rule on an individual basis, in writing and containing all conditions to such exception, or by policy. This limitation does not apply to those employees assigned to Divisions in which the capturing of digital images or recordings is specifically part of the employee's duties, such as Information Outreach, Special Enforcement Division, Fire Marshall and Inspectors, Training, or Emergency Management or those operating under the express direction of such authorized individuals.

1.1 Ownership of Media Created On-Duty. All images and recordings taken by on-duty personnel during the course of their duties are UFA Owned Media, are the sole property of the UFA, are under the control of the Fire Chief or his/her designee, regardless of the storage location, and may only be distributed by or with the approval of the Information Outreach Division. Such images and recordings are considered to be taken within the scope of employment pursuant to copyright law as a work made for hire. This specifically includes any images or recordings taken by an on-duty employee during the course of their duties with a non-UFA owned camera, cell phone camera, or any other digital imaging or recording device.

1.2 Use of UFA-Owned Device. All images and recordings taken by or stored on a UFA-Owned device, or removable storage, regardless of whether it was created while the employee was on-duty, are subject to review, duplication, use, or deletion by UFA. Employees will have no expectations of privacy for any images, recordings, or data of whatever kind created, contained, or stored on a UFA-Owned device. UFA-owned devices are subject to collection, inspection, and retention by UFA at any time and without notice.

1.3 Use of Personal Device: An employee using a non-UFA owned camera, video recorder, audio recorder, or the camera/video/audio function of a non-UFA owned cellular phone, or any other digital imaging device, while on-duty, to capture UFA Owned Media, may result in the device being subject to examination or forensic imaging for the purpose of records requests under GRAMA, litigation holds or discovery requests made under the Federal and Utah Rules of Civil Procedure, or other requirements related to investigations or legal obligations of UFA. In addition, the member must comply with all other aspects of this policy as if UFA Owned Media were taken with a UFA-owned device.

1.4 Retention and Production.

1.4.1 Preservation. Regardless of its storage location, UFA Owned Media must be preserved and not be deleted without the written permission of the Fire Chief or his/her designee, except as permitted by an applicable policy. UFA Owned Media will be subject to the UFA Records Retention and Litigation Hold policies. Any UFA-Owned Media that has evidentiary value, such as investigative photos, vehicular accidents involving UFA vehicles, fire scenes showing evidence of cause and origin, incident scenes showing the locations of victims, fire code violations, etc., should be flagged and documented with a chain of custody form to be kept with the data.

1.4.2 Production. Each employee who creates and retains UFA Owned Media is responsible for producing such images or recordings if needed for the purpose of responding to public records requests or legal document production. Employees should maintain and index the data in a manner that allows and facilitates its location in the event of a production requirement and respond promptly to any and all inquiries from the Records Manager or Chief Legal Officer to inquiries about the existence of any responsive documents.

2.0 PROHIBITIONS ON IMAGING AND RECORDING

2.1 Incidents. Unless specifically authorized pursuant to this Policy, employees are prohibited from using a video recorder, helmet camera, audio recorder, or the camera/video/audio function of a cellular phone, or any other digital imaging or recording device while responding to, operating at, or returning from, any incident. Any employee who inadvertently takes such an image at an incident scene must report the fact through the chain of command to the incident commander at the earliest possible opportunity. Employees will not be subject to discipline for inadvertent violations that are duly reported.

2.2 HIPAA. Except for those expressly authorized to do so as part of their duties, employees are prohibited from creating photographs, video, recordings, or imagery containing individually identifiable patient information covered by the Health Insurance Portability and Accountability Act (HIPAA) and state privacy laws. Any employee who inadvertently creates such data, should immediately report the fact through the chain of command and the information will be either deleted or handled pursuant to the HIPAA Privacy Rule and UFA's HIPAA policies (i.e. protected in the same manner as patient care reports and medical documentation). Employees will not be subject to discipline for any inadvertent violation of this subsection that are duly and immediately reported.

2.3 Individual Privacy. Employees are prohibited from taking any images of another person, including other UFA employees, in any location where the person has a reasonable expectation of privacy, including a bathroom, restroom, bedroom, hotel room, locker room, changing area, or any other location where a reasonable person would believe that he or she could disrobe in privacy, without being concerned that his or her undressing was being photographed, filmed, or video recorded by another; or a place where one would reasonably expect to be safe from hostile intrusion or surveillance.

2.4 Residences. Employees are prohibited from taking any images of another person in that other person's residence without that person's consent. Any employee who inadvertently takes such an image must immediately report the fact through the chain of command. Employees will not be subject to discipline for any inadvertent violation of this subsection that are duly and immediately reported.

3.0 ACCEPTABLE CAPTURE OF DIGITAL IMAGES AND RECORDINGS

3.1 Authorized Personnel. Employees whose position requires the capturing of images or recording for their job duties, such as Special Enforcement Division personnel, Fire Marshall and Inspectors, Training Division personnel, Public Information Officers, Safety Officer, or Chief Officers, are exempt from the restrictions in this Policy. Such employees should still comply with the retention and production requirements of this Policy and with the general privacy and HIPAA restrictions of Subsections 2.1 through 2.3 unless capturing such data is strictly necessary to proper satisfaction of a job duty (such as documenting a potential crime scene).

3.2 Authorized Recording On-Scene. In addition to the authorizations provided for in this Policy and subject to the restrictions and procedures stated herein, a Captain, Battalion Chief, Operations Chief, or Assistant Chief may record digital images, video, or audio recordings for the purpose of incident documentation, collection of evidence, training, investigations, and/or public relations purposes.

They may also specifically direct another employee to do so for the same purposes.

3.2.1. Appropriate Personnel. If an image or recording created pursuant to this Subsection was not captured for use by the individual taking the image or recording, it should be, as soon as is practicable, sent to the appropriate individual (i.e. investigator, training, Command, or PIO). An Incident Commander or the Fire Chief may prohibit the taking of imagery at a given scene based upon the circumstances.

3.2.2. Personal Device. If such an image or recording is captured on a personal, non-UFA-owned device, once the transfer provided for above has been completed, the employee should delete the data from the personal device unless permission is granted for use of the image or recording by the appropriate individual pursuant to Subsection 4.0.

3.3 Non-interference. The capture of digital images or recordings allowed under this Policy must not interfere with or delay operational activities, except to the extent that imagery related to cause and origin may require overhaul to be delayed for a reasonable period.

3.4 Automatic Recording Devices. Some UFA vehicles may be equipped with video or audio recording devices that begin to record automatically upon initiation of lights and/or sirens. Employees may not delete, alter, or cease operation of these recordings in an effort to obfuscate or impede inquiry or investigations. All data from automatic recording devices will be downloaded by designated personnel and managed pursuant to Subsection 4.0 of this Policy. Once downloaded the data should be deleted from the local device or removable memory storage.

3.5 Unmanned Aerial Vehicles. Digital data, imagery, or recordings obtained from the use of an Unmanned Aerial Vehicle ("UAV") must be downloaded by designated personnel as soon as practicable following the conclusion of the incident in which the UAV is used. Once downloaded, the data should be deleted from the local device or removable memory storage.

3.6 Personal Photos. This Policy does not apply to, and the media will not be considered UFA Owned Media, photos taken by on-duty personnel with a personally owned device for purely personal and non-business purposes, such as photos of friends and family members during a fire station visit or co-workers posing for a group photo.

3.6.1 Images or recordings taken pursuant to this exception must not violate the privacy provisions provided for herein and may not contain content that would violate any policy related to discrimination or harassment. Images taken pursuant to this exception shall not be used for political or commercial purposes in any manner that expressly or implicitly indicates an endorsement by the UFA.

3.6.2 Any image or recording created pursuant to this personal exception that captures business related matters of the UFA that would make it subject to a public records request will cause it to be considered UFA Owned Media and must comply with this Policy.

4.0 USE AND RETENTION OF DIGITAL MEDIA

4.1 Use of Images and Recording. Images and recordings captured pursuant to this Policy must be used for appropriate, mission and job-related purposes. They should not be used, printed, copied, scanned, e-mailed, texted, forwarded, posted, uploaded, shared, reproduced or distributed in any manner, except as provided in this Policy.

4.2 Posting on Social Media. The posting of UFA Owned Media on personal web sites or social media such as Facebook, Instagram, Snapchat, Twitter, Tiktok, or YouTube is prohibited, except as official communications by authorized members of the Information Outreach Division or Command Staff. Credit for capturing the images or recordings will be provided if appropriate. If UFA Owned Media created by operational personnel are posted as official communications, the individual who captured the media may then repost such media on personal social media. The Information Outreach Division may also authorize the distribution of UFA Owned Media not used in official communication on personal social media on a case-by-case basis. Employees should not post UFA Owned Media to personal social media prior to such authorization.

4.3 Integrity of Media. UFA Owned Media stored on devices or in any centralized repository may not be materially altered via any software product or utility such as Photoshop, unless authorized and/or express permission is granted by the Fire Chief or his/her designee. If permission to alter a photo is granted, the original photo shall not be altered in any way, and any copies that are altered shall be appropriately identified and documented as to being an altered copy. The details of the alteration including what was altered, the identity of the employee performing the alteration, and the time and date of the alteration, must be noted and preserved.

4.3.1 The requirements of Section 4.3 are not applicable to standard image improvement processes used to make images more presentable for

distribution such as the application of filters or color correction. However, those applying such effects should retain a copy of the original image if practicable.

New policy dated: June 9, 2021