

# IDAHO STATE POLICE PROCEDURE

## 02.05.04 DIGITAL ASSETS

### I. Purpose

This procedure establishes guidance for the collection, use, retention, and release of photographs and videos created during Idaho State Police (ISP) operations. Digital assets may be used to inform the public, support public safety education, document agency activities, and promote community outreach while protecting investigative integrity, privacy interests, and public safety.

All public releases of digital assets must comply with [ISP Procedure 02.05 – Public Affairs and Communications](#), including the provisions governing authorized and prohibited information for release.

### II. General Principles

- A. ISP employees shall treat all individuals involved in incidents with dignity and respect when capturing or releasing digital assets. Because many law enforcement incidents involve trauma or sensitive circumstances, personnel shall exercise sound judgment when photographing, recording, or publicly releasing digital assets.
- B. Public safety, officer safety, and investigative integrity shall remain the primary priorities during any incident.
- C. Digital assets that constitute evidence shall be preserved in accordance with applicable law and procedures. Exceptions may apply as outlined in [EHF 08.08 - Social Media for Undercover Operations](#).

### III. Collecting Digital Assets

- A. Digital assets can be captured in public settings without gaining express permission from those viewed.
- B. When digital assets prominently feature a specific individual, permission should generally be obtained before public release.
  - 1. In public settings, permission may be verbal.
  - 2. Written permission is preferable when practical.
- C. When a child is the primary subject of a digital asset, express verbal permission from a parent or guardian must be obtained from that individual, unless taken in a public setting.
- D. When digital assets are taken at schools or daycare facilities, employees should confirm that the institution has a valid photo release for the students included.

## IDAHO STATE POLICE PROCEDURE

- E. When feasible, personnel should announce their intention to gather digital assets for public release and allow individuals who object to move out of view.

### IV. Incident Scene Photography

- A. Digital assets captured at crash scenes should focus on the public safety response and impact of the incident.
- B. In general, digital assets should mainly focus on:
  - 1. ISP response vehicles and personnel.
  - 2. Traffic impacts such as lane closures or detours.
  - 3. Emergency response or cleanup operations.
- C. Digital assets shall avoid identifying individuals or involved vehicles.
- D. Except in rare circumstances, digital assets intended for public release should be taken from locations accessible to the public.

### V. Releasing Digital Assets

- A. When practical and appropriate, digital assets intended for public release shall be reviewed by a supervisor or the Public Affairs Office (PAO).
- B. Digital assets should support legitimate agency purposes such as:
  - 1. Public safety education.
  - 2. Community outreach.
  - 3. Incident notification.
  - 4. Recruitment or agency awareness.
- C. Digital assets captured within restricted crime scenes are generally considered evidentiary and should not be released unless approved through the chain of command or the PAO.
- D. ISP may choose not to release digital assets of fatal or serious injury incidents.
- E. When digital assets are released to assist an investigation, such as identifying a suspect or vehicle, the release shall be approved through the chain of command and coordinated through the PAO.
- F. Digital assets obtained from other agencies or individuals shall not be released without their permission and appropriate credit.

### VI. Editing and Watermarks

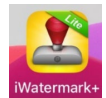
- A. Digital assets released through official ISP platforms should incorporate alternative and descriptive text when practical to support accessibility compliance.

## IDAHO STATE POLICE PROCEDURE

- B. Digital assets may be edited to protect privacy or remove identifying information when appropriate.
- C. In general, only minor edits like cropping, blurring, or redaction may be used to remove:
  - 1. Identifiable license plates.
  - 2. Identifying vehicle markings.
  - 3. Faces of uninvolved people.
  - 4. Commercial or identifying branding of an involved party.
  - 5. Other sensitive information.
- D. The ISP watermark or logo may be applied to digital assets to identify the source of the image.

### VII. Approved Phone Applications

- A. Approved applications or software may be used to edit digital assets for public release, including the application of watermarks, redactions, or blurring:
  - 1. iWatermark+ – to apply ISP watermark branding
    - a. ISP logo should be in the lower right corner with 100% transparency.
    - b. The asset itself may necessitate adjustments to logo transparency or placement.
  - 2. Blur Photo – to blur identifying information.
- B. Editing tools and approved applications may be designated by the PAO or by Information Technology Systems, as appropriate.
- C. Editing shall comply with Section VI of this procedure.



# IDAHO STATE POLICE PROCEDURE

## Photo Examples

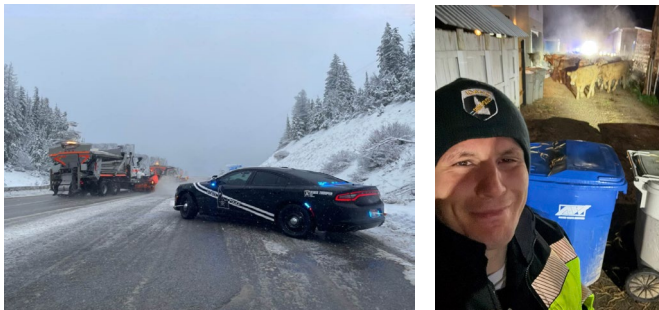
### 1. Crash Scene



### 2. Enforcement



### 3. Extraordinary Incidents



### 4. Community Events & Employee Highlights

