OXFORD POLICE DEPARTMENT

GENERAL ORDER 3.11

Internet, Computers, Social Media & Email

ISSUE DATE: February 1, 2015 ISSUED BY:

EFFECTIVE DATE: February 29, 2016

AMENDMENT DATE: Chief of Police, Joey East

City of Oxford Employee Handbook: Section 15, Information Technology
Standard Reference(s): 82.2.5, MSLEAC 3.13, 3.14

Warning: This directive is for departmental use only. This general order should not be construed as a creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this general order will form the basis for departmental administrative sanctions. Violations of the law will form the basis for civil and/or criminal sanction(s) in a recognized judicial setting.

PURPOSE

The purpose of this policy is to establish oversight concerning personal web pages, internet sites, and email when referencing the Oxford Police Department: to ensure employees use appropriate discretion in the use of references to the Oxford Police Department so as not to discredit or disrespect the department; to ensure that the release, either directly or indirectly, of information concerning crimes, accidents, or violations of ordinances or statutes to persons outside the department is not disseminated; and that all employees treat as confidential the official business of the department. Professionalism, ethics, and integrity are of paramount importance in the law enforcement community, therefore, to maintain the public's highest level of respect, we must place reasonable restrictions on our conduct and appearance, and hold to these standards of conduct whether on or off duty. An employee's actions must never bring the department into disrepute, nor should conduct be detrimental to its efficient operation.

POLICY

Employees of the Oxford Police Department have a right to have personal web pages or sites. When reference is made to or about the Oxford Police Department, a review of that reference is needed to ensure that such reference does not compromise our integrity and thus, undercut the public confidence in this agency or this profession. Therefore, it shall be the policy of the Oxford Police Department that employees of the department are prohibited from posting, transmitting and/or disseminating any photographs, video or audio recordings, likeness or images of department logos, emblems, uniforms, badges, patches, marked vehicles, equipment, or other material that specifically identifies the Oxford Police Department, on any personal or social networking website or web page, without the express written permission of the Chief of Police. (MSLEAC 3.13)

No employee shall represent themselves, directly or indirectly, in any public forum as a member of the Oxford Police Department, either by text, photograph, or image depicting the uniform, badge, or patch, in any manner that reflects a lack of good moral character. No employee will represent themselves in any public forum as an employee of the Oxford Police Department with other information, opinion, or posture that would bring unfavorable criticism or embarrassment upon the department or provide information that would compromise or provide results of an on-going and/or completed criminal, administrative or other departmental investigation. Employees should also refer to the Oxford Police Department Code of Conduct, Policy 2.11, insubordination, and listing of violations.

I. Web based pages or postings

A. Employees having personal web pages or other types of internet postings which can be accessed by the public or by granted permission, shall not place or allow photographs or depictions of themselves dressed in uniform and/or displaying official identification, patches or badges, or in any other way, either directly or indirectly, identify themselves as an employee of the Oxford Police Department for any reason, without approval as indicated in this directive.

1. Photographs or other depictions of department uniforms, badges, patches, or marked units shall not be posted on internet sites without the approval of the Chief of Police.
2. Photographs of the inside of the police building as well as any crime or accident scene shall not be posted.

3. Employees are prohibited from posting, transmitting, and/or disseminating any pictures or videos of official department training, activities, or work-related assignments without the express written permission of the Chief of Police.
4. Employees wishing to use photographs, depictions, or references to the Oxford Police Department must receive approval from the Chief of Police.
5. Employees who post photos, comments, etc. of other department employees must inform and seek approval from the employee(s) before posting same.
6. Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provisions of this policy shall notify his or her supervisor immediately for follow-up action.
7. Sites deemed inappropriate, whether an employment association or not, bringing discredit to this department or to a department employee, or promoting misconduct, whether on or off duty, may be investigated through a criminal or administrative investigation.
8. All employees shall treat as confidential the official business of the department. Employees should refer to the Oxford Police Department Code of Conduct, Policy 2.11 and other policies regarding releasing information that is protected.
9. No employee shall release, either directly or indirectly, information concerning crimes, accidents, or violations of ordinances or statutes to persons outside the department.
10. No employee shall reveal any unauthorized information to any person not a member of the department or authorized to receive such information.
11. No employee shall gossip about the affairs of the department with persons outside of the department.
12. If an employee indicates in any public forum any opinion on a police related issue, then that employee shall state that the views and opinions expressed are the employee's personal ones, and not those of the Oxford Police Department.

B. Approval Process

An employee seeking approval to use references to the Oxford Police Department on a personal website, web page, or other public forum, shall submit a request for approval to the Chief of Police via the chain of command.

1. The request shall describe the proposed reference and purpose.
2. A list of the reference and any media to be used shall be provided.
3. A printed layout of the entire web page, posting or site shall be provided.
4. The employee will receive an approval or denial of the request.
5. Any changes made to a previously approved posting must be submitted for reconsideration.

C. Limitations

1. No sexual, violent, racial, ethnically derogatory material, comments, pictures, artwork, video or other reference may be posted along with any department approved references.
2. Employees shall not post any material on the internet that brings discredit to or may adversely affect the efficiency or integrity of the Oxford Police Department or otherwise compromises and/or state the results of any ongoing or completed criminal, administrative or other departmental investigation.
3. Employees should consider the possible adverse consequences of internet postings, such as future employment, cross-examination in criminal cases and public as well as private embarrassment.
4. Employees are reminded to exercise good judgement and demonstrate personal accountability when choosing to participate on social-networking sites.

II. EMAIL Policy

It is the policy of the Oxford Police Department to authorize certain employees the use of department email accounts for the conduct of official law enforcement business. Approval and authorization to use such email systems is the responsibility of the Chief of Police. Employees authorized to use department email accounts shall only do so within the scope of their law enforcement duties and responsibilities and within the professional guidelines established in this policy.

1. Employees of the Oxford Police Department may be authorized by the Chief of Police as recipients of an email account administered by the department's network system. Such email accounts allow for the sending and receiving of email messages internally, as well as from outside the Oxford Police Department via the internet.
2. Employees are prohibited from causing, receiving, displaying, printing or otherwise disseminating material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating, or defamatory. Any employee encountering such material shall report it to his or her supervisor immediately. The supervisor shall then report the incident to the Chief of Police following established procedures.
3. Employees are prohibited from using the Oxford Police Department computer equipment or email accounts to transmit or receive destructive programs (i.e., computer "viruses") or for any other unauthorized use. (MSLEAC 3.14)
4. Email messages, both sent and received using departmental equipment, are department property, and should not be considered private. Casual or improper use of email can create a liability to the Oxford Police Department from

both employees and the public. All information, data, and emails are to be considered public information through the Freedom of Information Act. All users should be aware that while it is not the practice of the Oxford Police Department to routinely monitor email messages, messages may be monitored from time to time, without notice, as deemed necessary by the Chief of Police. See also the City of Oxford Information Technology Policy, Section 15.

5. Employees shall not participate in email chain letters, "mail bombs", "spamming", or other activities that generate a large amount of useless network traffic.
6. Users must ensure that they do not divulge information of a sensitive or confidential nature while using the email system. Employees should use reasonable care to ensure that the intended recipient will be the one to have access to the message.
7. As a required work tool, employees assigned a departmental email account will check their messages at least once per shift. Employees should also check their email accounts near the end of their shifts prior to regularly scheduled days off to ensure prompt action of priority messages.
8. Good customer service is expected, and as such, email messages requiring a response or action from an employee will be handled as soon as practical. Email messages left on an employee's day off will be returned on the next duty day if possible.
9. When an employee is unavailable for more time than their regularly scheduled days off, such as for vacation, training, or other time off, the "rules" function of the Outlook email program will be enabled to notify persons attempting contact of the scheduled absence. The reply message displayed from the "rules" function should include an anticipated date of return and an alternate point of contact for issues requiring immediate attention.
10. See City of Oxford, Employee Handbook, Information Technology Policy, Section 15

PRECAUTIONARY STATEMENT TO MEMBERS

Wireless Voice/Data Communications is one of the most rapidly changing technologies today. As such, policy development and acceptable procedures are constantly being adjusted in an attempt to keep up with these changes. Members are cautioned that while this policy may not directly address all issues related to the use of these technologies; sound and legal use of these devices must be paramount.

The use of either Department or personally owned wireless devices to record images or audio comes with certain requirements in order to safeguard both the member and the Department from wrongful claims. It is important to consider that the use of personal equipment, while acting in an official capacity as a law enforcement officer, may subject that equipment to both subpoena and public record review. This not only includes the recording device, but may also include any personal computer or audio visual equipment used to access, store or review the recorded material. Wireless communications of any kind that address official public business, even if communicated over a personal device, are subject to public record laws and record retention provisions.

III. Wireless Telephone Use (MCD and EMD's)

Wireless telephones as addressed in this order include hand-held and/or vehicle mounted radio devices that wirelessly connect to telephone networks for two-way voice and possibly data services. Wireless telephones include and are referred to under a variety of names and descriptions, i.e., cellular telephone, smart phone, Blackberry, Droid, or Windows Mobile device, personal data assistant (PDA), mobile communicating device, electronic messaging device.

It is the policy of the Oxford Police Department to permit the use of wireless voice/data communication devices. While it is understood that the authority to carry a personal cellular telephone or other wireless voice/data communications device on-duty or during work related functions is a convenience, anyone choosing to carry one of these devices must comply with the stipulations set forth in this policy. Violations could result in the loss of this convenience and/or disciplinary action.

A. Use in Patrol Vehicles

The use of cellular phones while operating a police vehicle can cause distractions that could result in injury to the operator, the public, and cause damage to the vehicle. It is strongly suggested that when cell phone use is required, the operator of the motor vehicle park in a safe location to complete the conversation, and not do so while the vehicle is moving through traffic.

1. Employees should not use wireless telephones for voice communication while driving a Patrol vehicle, or any other vehicle, while on Patrol business unless the telephone is used in a hands-free mode.
2. Employees will not use wireless telephones for data communication, i.e., reading, composing, sending or manually accessing text messages, e-mail, or Internet functions while driving a Patrol vehicle or any other vehicle while on Patrol business. This policy does not prohibit officers from using a Mobile Computer Device (MCD) to check license plates of vehicles or handle routine short transactions with command keys while driving.
3. Officers will not use wireless telephones while driving a Patrol vehicle in a pursuit or emergency response mode.
4. Use of wireless telephones in Patrol vehicles for personal calls should be limited to regular break times. Such use of Patrol wireless telephone equipment is further restricted as outlined elsewhere in this order.

Wireless telephones will not be routinely used in lieu of the Patrol radio to conduct Patrol business, i.e., calling wreckers or ambulances.
Use of personally owned wireless telephones for personal calls at the workplace should be limited to regular break times and may further be restricted in accordance with this and other directives.
Employees will not allow the wireless telephone to interfere with their duties and responsibilities. Answering the Patrol radio and conducting regular Patrol duties will take priority over use of the wireless telephone.
Personal communications on cellular telephones or other wireless communication devices while in uniform or engaged in enforcement activity shall be brief in nature, and conducted out of the view of the public, unless exigent circumstances exist.

IV. Computer Policy
The department computer system is intended solely to aid and assist employees in the performance of their assigned responsibilities. Employees therefore, will limit their transactions and activities to necessary assigned responsibilities. Security clearance and access to information is restricted to official business and does not permit employees to access information for personal reasons, financial gain, or unauthorized distribution. Any misuse of the department computer system is grounds for disciplinary action, and or criminal prosecution. Access to NCIC, State, or other department files is restricted to authorized *entries, modifications, research, investigations,* and *inquiries.*

Use of information:
Much of the information obtained through law enforcement computer systems is **confidential, restricted** or sensitive data which must be carefully controlled to ensure compliance with applicable local, state, and federal guidelines. Any employee accessing files or obtaining information from law enforcement systems is accountable for the appropriate and correct use of the information.

Some sensitive information in our computer or hardcopy files can only be accessed by authorized individuals having a *need to know.* If you have a doubt about your authorization to access certain data, check with your supervisor, before accessing the information. These records normally include *internal affairs, personnel, and intelligence*, and *undercover operations* files.

Responsibility:
Employees who use department computers are accountable for proper operation, and each transaction. The computer system administrator will track entries; recording the time, date, person making the entry, and the file entered. Employees operating the system will exercise reasonable care of the equipment, and are responsible for damage resulting from intentional abuse or negligence.

V. Software Guidelines:
Under no conditions, will software that has not been reviewed and approved for departmental use be loaded onto departmentally owned or operated computers.

This includes any demonstration software, sample software, Internet access free software, shareware, or other free programs. Software that does not meet this requirement and is loaded on a computer shall be immediately removed. (82.1.7)

In compliance with software piracy laws, no software from this agency may be removed from the premises or copied for personal use. No software may be brought into this department and installed into agency computers without the express written permission of the Chief of Police or designee. When permission is obtained, the software will be installed by a qualified individual, in accordance with licensing agreements. Requests for new software may be made through the office of the Chief of Police or designee. If approved, the software will be purchased and registered to the agency.

Software installed on individual computers is subject to review at any time. Unauthorized software will be removed. No unauthorized personnel are to be allowed access or use of departmental computers in the agency or in homes of employees.

Users will not disable or uninstall virus protection software on departmental owned computers.

VI. Laptop/MDT/IPad Guidelines:
Laptop computers are very vulnerable to theft and require extra diligence in safeguarding for travel. Following are guidelines to be followed when department laptops are carried outside of the department:

1. Always carry the laptop in its specially padded carrying case.

2. When traveling by air, always carry the laptop on the airplane. Never check the laptop as baggage and never put the laptop inside another case checked as baggage. The only exception to this is that a laptop can be shipped in a special shipping container with padded foam for shipping sensitive electronic items.
3. Always hand-carry the laptop when traveling to and from the airport. Don't put it in the trunk of a cab or on the rack of an airport shuttle.
4. Always make sure that there is no flash drives in when moving from place to place.
5. If you carry a computer home to work on agency projects, the computer will be carried to and from the office on a daily basis during the workweek. Under no circumstances will Oxford, Mississippi Police Department property be left at your residence while you are at work without express the express permission of Chief of Police.
6. Laptop/IPad computers may be assigned individually or signed out at departmental discretion as approved by of Chief of Police
7. Employees will not alter or disassemble any equipment, device or connection to a MDT terminal, modem, transmitter or any other component of the MDT (computer) system without the consent of the Chief of Police or the System Administrator.
8. Employees assigned a vehicle containing a MDT (computer) will be responsible for the physical security and general upkeep of that MDT (computer). Any requests for repair, maintenance, technical support or training should be forwarded through the appropriate chain of command to the System Administrator.
9. All employees will use every reasonable precaution available to keep the MDTs (computer) secured (locking the vehicle when unattended).
10. In order to protect the MDT's (computer) internal addressing/formatting, the MDT (computer) should be physically turned off (programs exited, unit signed off and powered down) if the vehicle must be jump started.
11. All vehicle radios and MDTs (computer) should be turned off (programs exited, unit signed off and powered down) when the vehicle is placed out of service.
12. All personnel using MDTs (computer) are responsible for signing on at the beginning of their tour of duty and signing off at the conclusion of their tour of duty.
13. Employees have no expectation of privacy of information contained in any MDT (computer), LAN terminal or departmental computer. Any computer system security feature such as passwords or message delete functions do not affect the rights of supervisors, the System Administrator or the Chief of Police or his designee to access information at any time for business purposes. When requested by a supervisor in their chain of command, an employee is required to disclose any passwords or codes necessary to access their computer.

Any hardware enhancements, peripheral, or additions to department or city-owned equipment must be approved by the Chief of Police or the appropriate representative of the city. The Assistant Chief of Police is responsible for determining proper installation procedures.

The Dispatch Supervisor will assure hard drive files are routinely backed up on external media to assure information loss is minimized. Computer files maintained by the OPD will be backed up on a regular basis and are stored at various locations to ensure minimum loss in case of fire, floods, or other emergencies. (82.1.6 a, b)

Prohibited Activities

1. Using computer or network services for commercial purposes or for profit.
2. Knowingly installing or running a program that will damage or place an undue burden on the system.
3. Knowingly acting in a manner that will disrupt normal operations of computers or the network.
4. Using computer or network services in a way that violates copyrights, patent protections or license agreements.
5. Gaining unauthorized access to information that is private or protected, or attempting to do so.
6. Attempting to identify passwords or codes, interrupting security programs, or attempting to do so.
7. Reading, copying, changing or deleting another person's work.
8. Using another person's user/id/password, or allowing others to use yours.
9. Attempting to gain system and/or network privileges to which you are not entitled.

OXFORD POLICE DEPARTMENT

GENERAL ORDER 4.24

Mobile Video

ISSUE DATE: February 1, 2016 ISSUED BY:

EFFECTIVE DATE: February 29, 2016

AMENDMENT DATE: Chief of Police, Joey East

Standard Reference(s): 42.2.1(c), 83.1.2, 83.2.1, 83.2.2, 83.2.3, 83.2.4 (a-d), 83.3.1, 83.3.2 (a-e), 84.1.1(a-g), 84.1.2, 84.1.3, 84.1.4, 84.1.5, 84.1.6 (c,d), 84.1.7

Warning: This general order is for departmental use only. This general order should not be construed as a creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this general order will form the basis for departmental administrative sanctions. Violations of the law will form the basis for civil and/or criminal sanction(s) in a recognized judicial setting.

POLICY:
It is the policy of the Oxford Police Department that officers will use the MVR equipment to record (both audio and video), in their entirety, interactions between officers and the public as described in this directive. To maximize the utility of this equipment, officers will follow the procedures for MVR equipment use as set forth in this directive. The use of mobile video equipment (MVR) provides persuasive documentary evidence and helps defend against civil litigation and allegations of officer misconduct. Officers assigned the use of these devices shall adhere to the operational objectives and protocols outlined herein so as to maximize the effectiveness and utility of the MVR and the integrity of evidence and related video documentation.

Definitions

1. Recorded Media — Refers to audio-video signals recorded on any of several storage devices, including analog tape (VHS, SVHS, Hi 8mm), digital tape (DV), or other portable digital storage devices (CD, DVD, hard drive, etc).

2. In-Car Video/Audio Systems (MVR) — This refers to any system that captures audio and video signals capable of installation in a vehicle, and that includes at minimum, a camera, microphone, recorder, and monitor. This also refers to the wearable digital camera systems issued on a permanent or temporary basis to individual officers.

3. MVR Technician — Personnel trained in the operational use and repair of MVRs, duplicating methods, storage and retrieval methods and procedures, and who possess a working knowledge of video evidentiary procedures.

PROCEDURES
Operating Procedures

MVRs are utilized to accomplish the following objectives:

1. Enhance officer safety;
2. Accurately capture statements and events during the course of an incident;
3. Enhance the officer's ability to document and review statements and actions for both internal reporting requirements and for courtroom preparation/presentation;
4. Provide an impartial measurement for self-critique and field evaluation during recruitment and new officer training;
5. Capture visual and audio information for use in current and future investigations.

Officers will adhere to the procedures listed below when utilizing MVR equipment.

1. MVR equipment installed in a vehicle is the responsibility of the officer assigned to that vehicle and will be maintained according to manufacturer's recommendations.

2. Prior to and throughout each shift, officers will ensure that all components of their MVR equipment are working satisfactorily and will bring any problems to the attention of a supervisor immediately.
3. MVR equipment will automatically be activated when the vehicle's emergency warning devices are in operation. The equipment may be manually deactivated during non-enforcement activities such as protecting accident scenes from other vehicular traffic.

Officers will ensure that MVR equipment (both audio and video) is activated and operating properly and that the video recorder is positioned and adjusted when feasible to record events in the following circumstances:

1. Record the reason for their current or planned enforcement action, such as traffic stops or DUI observations;
2. Record the actions and/or statements of suspects if the recording would prove useful in later judicial proceedings. For example, interviews, sobriety performance tests, while in custody or during transportation.
3. Record the circumstances at crime and accident scenes or other events such as the Confiscation and documentation of evidence or contraband;
4. Record motorist assist, disabled vehicles and abandoned vehicles.
5. Record the audio portion of a conversation with a citizen.

Officers using digital recording devices will ensure there is adequate storage on the media device.

Officers will note in offense, arrest, and related reports when video/audio recordings were made during the incident in question.

Officers shall only use data storage devices as issued and approved by this agency.

Officers will not erase, alter, or tamper with MVR tapes.

Mandatory Recording Officers must comply with all applicable laws and departmental policy when a person is contacted or a suspect is interviewed utilizing a video or audio recording device. When the MVR is activated, officers shall ensure that the audio portion is also activated so all events are properly documented. Officers are encouraged to narrate events using the audio recording, so as to provide the best documentation for pretrial and courtroom presentation (*Example: During a pursuit the pursuing officer may state/narrate that the suspect threw an object out the driver's window at a certain location)*. Officers shall use both audio and video components of the system during the following:

a. Traffic stops (to include, but not limited to traffic violations, stranded motorist assistance and crime interdiction stops).
b. Priority response to calls-for-service (code responses).
c. Vehicle pursuits.
d. Crimes in progress.
e. Prisoner transports of subjects who are combative, violent, claim injury, or are behaving in such a way additional charges or complaints will likely result.

Discretionary Recording Any situation or incident that the officer, through training and experience, believes should be audibly and visually recorded to include any violations or misdemeanor crimes in progress or statements of witnesses/victims/suspects. Officers may cease recording (audio and/or video) should a traffic stop evolve, i.e., for the development of confidential information.

Field Training Officers will be responsible for training new officers in the operation of MVR equipment and will document the training.

MEDIA CONTROL AND MANAGEMENT – Digital Media

1. MVR does not require a chain of custody to hold evidentiary value.
2. No recorded media containing evidentiary value shall be destroyed, altered or erased unless an order of destruction is given by the court.
3. Recorded media with a signed destruction order from the court shall be erased and reused or destroyed.
4. Recorded media with administrative value only shall be stored by the shift supervisor, internal affairs or the Chief of Police or his designee.

Recorded media may be duplicated for court, investigative, training, or other purposes authorized by the Chief of Police or his designee.

All MVR recording are property of the Oxford Police Department and shall not be released to anyone. Anyone other than the officer that made the tape, a supervisor, internal affairs, or officer of the court requesting a MVR shall make the request to the Chief of Police. The request shall be in writing stating the reason for the request and proposed use of the recording. The Chief of Police will determine if the tape shall be released.

Request for MVR for civil actions shall be made by subpoena.

SUPERVISORY MEDIA CONTROL AND MANAGEMENT RESPONSIBILITIES

Personnel who supervise officers using MVR equipment will ensure that:

1. Storage devices are issued to officers upon their request.
2. Adequate number of new or erased storage devices are available.
3. Whenever an officer notifies a supervisor of a MVR devise that is not working properly or is in need of repair, the supervisor will determine if that unit shall be utilized. The supervisor shall notify the Assistant Chief or designee in writing with a description of problem and/or repairs that need to be made.
4. Whenever an officer has a citizen complaint that supervisor shall request the recorded media from the officer and review the content that is applicable to the complaint. The supervisor shall determine if there is reason to initiate an investigation. The recorded media shall be secured by the supervisor for administrative value until it is no longer needed by the supervisor, internal affairs, and/or the Chief of Police for its administrative value. The recorded media shall be turned over to the Chief of Police or his designee for administrative uses if requested.
5. Supervisor shall respond to the scene of any departmental shootings and departmental motor vehicle crash. The supervisor shall remove the recorded media and secure it according to department policies governing evidence or administrative matters.

OXFORD POLICE DEPARTMENT

GENERAL ORDER 4.28

Body-Worn Cameras

ISSUE DATE: February 1, 2016 ISSUED BY:

EFFECTIVE DATE: February 29, 2016

AMENDMENT DATE: Chief of Police, Joey East

Standard Reference(s): 42.2.1(c), 83.1.2, 83.2.1, 83.2.2, 83.2.3, 83.2.4 (a-d), 83.3.1, 83.3.2 (a-e), 84.1.1(a-g), 84.1.2, 84.1.3, 84.1.4, 84.1.5, 84.1.6 (c,d), 84.1.7

Warning: This general order is for departmental use only. This general order should not be construed as a creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this general order will form the basis for departmental administrative sanctions. Violations of the law will form the basis for civil and/or criminal sanction(s) in a recognized judicial setting.

PURPOSE:
This policy is intended to provide officers with instructions on when and how to use body-worn cameras (BWCs) so that officers may reliably record their contacts with the public in accordance with the law.

POLICY:
It is the policy of the Oxford Police Department that officers will activate the BWC when such use is appropriate to the proper performance of his or her official duties, where the recordings are consistent with this policy and the law. This policy does not govern the use of surreptitious recording devices used in undercover operations

PROCEDURES

A. Administration
The Oxford Police Department has adopted the use of the BWC to accomplish several objectives. The primary objectives are as follows:

1. BWCs allow for accurate documentation of police- public contacts, arrests, and critical incidents. They also serve to enhance the accuracy of officer reports and testimony in court.
2. Audio and video recordings also enhance this agency's ability to review probable cause for arrest, officer and suspect interaction, and evidence for investigative and prosecutorial purposes and to provide additional information for officer evaluation and training.
3. The BWC may also be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of evidence or contraband.

B. When and How to Use the BWC

1. Officers will activate the BWC to record contacts with citizens in the performance of official duties.
2. The BWC shall remain activated until the event is completed in order to ensure the integrity of the recording unless the contact moves into an area restricted by this policy.
3. If an officer fails to record the entire contact, or interrupts the recording, the officer shall document why a recording was not made, was interrupted, or was terminated.
4. Civilians shall not be allowed to review the recordings at the scene.

C. Procedures for BWC Use

1. BWC equipment is issued primarily to uniformed personnel as authorized by the Oxford Police Department. Officers who are assigned BWC equipment must use the equipment unless otherwise authorized by supervisory personnel.
2. Police personnel shall use only BWCs issued by this department. The BWC equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the Oxford Police Department.
3. Police personnel who are assigned BWCs must complete an agency approved and/or provided training program to ensure proper use and operations. Additional training may be required at periodic intervals to ensure the continued effective use and operation of the equipment, proper calibration and performance, and to incorporate changes, updates, or other revisions in policy and equipment.
4. BWC equipment is the responsibility of individual officers and will be used with reasonable care to ensure proper functioning. Equipment malfunctions shall be brought to the attention of the officer's supervisor as soon as possible so that a replacement unit may be procured.
5. Officers shall inspect and test the BWC prior to each shift in order to verify proper functioning and shall notify their supervisor of any problems.
6. Officers shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute in any manner BWC recordings without prior written authorization and approval of the Chief of Police or his or her designee.
7. Officers are encouraged to inform their supervisor of any recordings that may be of value for training purposes.
8. The department reserves the right to limit or restrict viewing the video file.
9. Requests for deletion of portions of the recordings (e.g., in the event of a personal recording) must be submitted in writing and approved by the Chief of Police or his or her designee in accordance with state record retention laws. All requests and final decisions shall be kept on file.
10. Officers shall note in incident, arrest, and related reports when recordings were made during the incident in question. However, BWC recordings are not a replacement for written reports.

D. Restrictions on Using the BWC

BWCs shall be used only in conjunction with official law enforcement duties. The BWC shall not generally be used to record:

1. Communications with other police personnel without the permission of the Chief of Police;
2. Encounters with undercover officers or confidential informants;
3. When on break or otherwise engaged in personal activities; or
4. In any location where individuals have a reasonable expectation of privacy, such as a restroom or locker room.

E. Storage

1. All files shall be securely downloaded periodically and no later than the end of each shift. Each file shall contain information related to the date, BWC identifier, and assigned officer.
2. All images and sounds recorded by the BWC are the exclusive property of this department. Accessing, copying, or releasing files for non-law enforcement purposes is strictly prohibited.
3. All access to BWC files must be specifically authorized by the Chief of Police or his or her designee, and all access is to be audited to ensure that only authorized users are accessing the data for legitimate and authorized purposes.
4. Files should be securely stored in accordance with state records retention laws and no longer than useful for purposes of training or for use in an investigation or prosecution. In capital punishment prosecutions, recordings shall be kept until the offender is no longer under control of a criminal justice agency.

F. Supervisory Responsibilities

1. Supervisory personnel shall ensure that officers equipped with BWC devices utilize them in accordance with policy and procedures defined herein.
2. At least on a monthly basis, supervisors will randomly review BWC recordings to ensure that the equipment is operating properly and that officers are using the devices appropriately and in accordance with policy and to identify any areas in which additional training or guidance is required.