OGDEN CITY POLICE
Office of the Chief

Policy No: 42

Subject Computers	Effective Date July 27, 2022
Department Police	Replaces Policy Dated July 13, 2022
Division All Police Personnel	Review Date May 2024
Authorized Signature Eric R Young	

NOTE: This rule or regulation is for internal use only and does not enlarge an officer's civil or criminal liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this directive, if proven, can only form the basis of a complaint by this agency, and then only in a non-judicial administrative setting.

I. PURPOSE

The purpose of this policy is to provide for the security and safety of computer equipment owned and issued by the Department and the data contained and transferred thereby.

II. POLICY

All computer equipment owned by the department will be operated to comply with Chapter 7-11 Sections D and E of the Ogden City Employee Policies and Procedures Manual and the State of Utah Criminal Investigations and Technical Services Act per Section 53-10 of Utah Code Annotated.

It is the policy of the Ogden City Police Department that employees will comply with all Federal, Utah State, and Ogden City laws, policies, user-agreements and guidelines when utilizing department-owned computers and electronics. This policy includes cellphones, tablets, mobile data terminals, and related electronic messaging devices that are utilized to access internal and external database services and information exchange networks. This policy includes devices owned by the individual only when they are used to access Federal, State or City databases.

III. PROCEDURE

A. Inventory and Location of Equipment

All mobile data computers will be inventoried by the authorized police department property custodian. In the case of mobile (laptop) computers this will be the Training Assistant in the capacity of property custodian. The property custodian, with assistance of the assigned technician from Information Technologies, will assist in the assignment, tracking and coordination of repairs to the computer. An inventory tracking log will be kept showing the current employee to whom equipment has been assigned and the location of each piece of equipment. Once assigned, the equipment is the responsibility of the department member until returned to the property custodian.

B. Physical Security

Mobile computers will be removed from the vehicle and placed in an area protected from excessive climatic extremes when the vehicle is unoccupied for extended periods of time. Mobile computers that must be left in vehicles during extremely hot conditions should be covered with a protective cloth.

If an assigned computer malfunctions during weekday business hours the employee may contact the IT technician at the Francom Public Safety Building or the 4th floor of the Municipal Building (#8747) for assistance. If the problem occurs after hours the employee responsible for the unit will call IT at #8747 and leave a message for the on-call IT technician with their name, the computer issue, and their contact number.

The computer should be positioned to prevent casual access to the information on the screen. During break or other periods of inactivity, the computer should have the screen closed.

C. Information Security

Records and information obtained from law enforcement databases, including the Bureau of Criminal Identification (BCI), National Crime Information Center (NCIC), Utah Criminal Justice Information System (UCJIS), Spillman, or similar systems are considered confidential and protected. Records and information contained in these databases will only be accessed, used, or distributed in the performance of legitimate police-related activities or investigations. Access, use, or distribution for any other purpose is forbidden and grounds for departmental discipline, up to and including termination. This includes leaving protected information, such as documents or computer databases, accessible to others when it is

reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal). All protected information that is printed shall be immediately destroyed after use by shredding or other effective means. Employees found in violation of this section might also face civil and criminal penalties. Misuse of UCJIS will fall sanction to UCA 53-10-108 and will be reported to the commissioner and the director of the Utah Bureau of Criminal Identification.

Passwords are to be changed as required and safeguarded to prevent unauthorized persons from gaining access. Operators are encouraged to change passwords frequently and in a random manner to avoid detection of passwords by others. Ogden City passwords will expire, and accounts will lock every 90 days. All other passwords should be changed every 45 days. Passwords are not to be given out to others, even those who have the same or greater access rights to the system. Operators are required to log off the various systems when leaving the computer terminals unattended in unlocked areas.

D. Storage of Information

Members are prohibited from storing protected information (including CJI) on electronic media devices.

E. Transfer of Information

The following will be followed during transfer of protected information (including CJI) in a physical media (printed documents, printed imagery, etc.) and/or a digital media format:

1. When removed from a controlled area (i.e., restricted area of the Department), the media is always within the possession of an authorized employee.

2. The media will only be delivered to, and left with, individuals or agencies who are authorized to be in possession of it.

3. If the media is delivered to an authorized agency and is not being left directly with an authorized individual, it will only be left in a controlled area of that agency's location which has been designated for such.

4. Physical media shall be destroyed after use by shredding or other effective means.

F. Software Ownership and Security

Only licensed software will be installed on a city issued computer. All software installations will be performed by the IT Department of Ogden City. Software purchased by the city is for installation and use only on the city owned computers for which it is licensed. It may not be installed or used on private computers or other city owned computers without proper license and authorization.

G. Data and Virus Protection

Each computer will be periodically scanned for viruses by IT using programs approved and purchased by the city. Removable media (flash drives, disks, removable hard drives, etc.) obtained from outside sources will not be installed or used in the computers without prior approval from the department. Removal of detected viruses can damage other information stored on the computer and therefore viruses should not be removed by anyone other than IT personnel.

H. Unauthorized Software Installation

No unauthorized, unlicensed, or unsuitable material will be installed. The computer will be periodically monitored by IT, a departmental designee, or a supervisor for the presence of unlicensed software or other unauthorized material. The presence of pornographic or other similar material may be grounds for disciplinary action.

I. Personal Conduct

The computer will not be used to distribute offensive or harassing statements, or to disparage others based on race, national origin, sex, sexual orientation, age, disability or political or religious beliefs. For the protection of the department and officers, an ongoing audit process will be conducted as all entries into any department computer system, including messaging and e-mail, may become legal documents and as such are subject to being subpoenaed. Inappropriate conduct will result in disciplinary action up to termination.

J. Equipment Maintenance and Care

Defects in the computer hardware and software systems should be documented and reported to the appropriate supervisor as soon as they are noticed. If an officer experiences a problem with the unit during regular business hours they may contact the IT technician at the Francom Public Safety Building or the 4th floor of the Municipal Building (#8747) for

assistance. If the problem occurs after hours the employee responsible for the unit will call IT at #8747 and leave a message for the on-call IT technician with their name, the computer issue, and their contact number. IT will facilitate a replacement computer. Maintenance may only be performed by those authorized by IT.

IT may direct the officer with the computer problems to leave the computer on the counter in the Duty Lieutenants' office at the end of their shift for repairs. The officer should place a note on the computer with their name, a description of the problem, and their contact number. IT will collect the computer and once it is repaired will return it to the Duty Lieutenants' office for the officer to pick it up.

The computer is to be kept free from dust, moisture, excessive heat and other damaging conditions. The screen should be cleaned with a soft cloth and a cleaner specifically recommended for computer screens. Keyboards and CPU cases should be cleaned with an appropriate cleaner. These will be provided for you and are to be kept in your vehicle. Abrasives should never be used.

All systems will be protected by an electric surge protector installed in the vehicle by Fleet.

K. Safety

Computers will not be used to obtain information while the vehicle is in operation. If it is urgent that you obtain the information while in transit, you must immediately switch to verbal communication through the dispatch center. If you receive a possible hit on an NCIC entry, i.e. wanted or missing person, stolen vehicle, stolen gun, you must switch to verbal communication through the dispatch center.

L. System Authorization and Password Requests

Requests for access authorization and passwords to the various systems within the department and CDS will be approved by the Division Commander.

M. Private Use of City Owned Equipment

Employees may not use city-owned computer equipment for private purposes.