CITY OF AKRON, OHIO

POLICE DIVISION

KENNETH R. BALL II, CHIEF OF POLICE

NUMBER P-2020-026	EFFECTIVE DATE July 23, 2020	RESCINDS P-11-026 Issued 10-31-11
SUBJECT Computer Equipment Procedure		ISSUING AUTHORITY Chief Kenneth R. Ball II

I. POLICY

Department computer systems and databases shall be used for law enforcement and work purposes only. Use of department computers, including email and internet access, shall comply with the City policy on employee use of email and internet. Members shall be aware that they have NO expectation of personal privacy in the use of the internet and any email systems when users utilize computers or services the police department provides. Technical Services Unit personnel may examine any documents or files on department issued computers for violations of this policy at any time.

Executive Order #02-2019, dated January 28, 2019, issued by the Mayor of the City of Akron, Ohio, on computer, electronic mail, Internet, and intranet usage outlines the City of Akron's policy for computer use. This procedure is to supplement the city's policy and provides additional guidelines.

II. DEFINITIONS

A. Computer resources – Includes, but not limited to: servers, workstations, stand-alone computers, laptops, printers, scanners, Mobile Data Terminals (MDT's), Mobile Data Browsers (MDB's), Personal Digital Assistants (PDA's), cell phones, tablets, software, data and all internal and external computer and communications networks (for example, Internet, e-mail, LEADS and other jurisdictions or agencies).

B. Computer data – Information that is being or has been prepared in a formalized manner intended for use in a computer system.

C. Computer virus – A computer program that copies itself into other programs stored in a computer with either a benign or negative effect.

D. Hardware – The computer and associated physical equipment directly involved in its presence.

E. Software – The programs and applications that control the functioning of the computer.

F. Shareware, freeware, open source – A method of distributing software programs whereby the programmer will allow anyone to use or share his programs for some specified period

of time with the expectation that the user will abide by the license which may include payment or registration.

III. PROCEDURE

A. HARDWARE

1. All hardware installed within this department is the property of the Akron Police Department and shall not be moved to any other location without the express authorization of the Technical Services Unit. This includes moving equipment within a particular unit from one location to another. ***Network data connections make it imperative that Technical Services personnel shall be the only ones to move the equipment.***

2. Employees are not to perform any maintenance on the hardware with the exception of cleaning or dusting of the exterior cases and cleaning of the monitor screen and keyboard.

3. No personal hardware (modems, cameras, PDA's, speakers, etc.) is to be installed without the approval of the Technical Services Unit.

B. SOFTWARE

1. The Akron Police Department will supply software to be used on department owned computers. No other software from any other source may be installed without the authorization of the Technical Services Unit. This includes, but is not limited to, software personally owned by employees or available in the public domain. Employees shall not remove departmental software applications from the Safety Division computers.

2. Software will be considered for installation by the department for employees who express a need. Such requests for software programs should be made in writing through the chain of command and approved by the Technical Services Unit. If the requested software is approved, the department will acquire, install and keep it in inventory.

3. Employees, except for authorized Technical Services personnel, shall not install software from one computer to another, nor are copies to be made for personal computers, notebooks, etc. without specific authorization from the Technical Services Unit. Software license agreements entered into by the City of Akron with all software providers must be observed.
4. Personnel shall not copy or otherwise create an image of any program or file purchased, used, or created by Technical Services personnel.

5. It is the policy of this department to abide by all software copyright agreements and to adhere to the terms of all software licenses to which the City of Akron is a party. Employees who violate any of the policies defined herein may be subject to the

appropriate criminal, civil, or departmental disciplinary action. Any employee who determines that there may be a misuse of software within this department shall notify their supervisor or the Technical Services Unit.

6. Current hardware and software technology offers the opportunity for some individuals to customize their workstations by displaying personalized backgrounds, screensavers, or by playing digitized sound or music. Some of these features could be construed as being offensive, suggestive, sexually oriented, or disruptive to the work environment by others. If there is any question concerning the appropriateness of any computer workstation display or sounds, the issue should be referred to the unit supervisor or the Technical Services supervisor, who will determine the suitability of the material in the work environment.

C. COMPUTER DATA

1. Employees should be aware that information on departmental computers could be subject to public records requests. However, some information is exempt from public records law and could violate departmental rules and regulations if disseminated. Public requests for information on a departmental computer should be referred to the Chief's office.

2. Personnel should save all documents/files to the G and H drives. In addition, personnel may store copies locally. Repairs to or replacement of workstations may cause total loss of data stored locally and may occur with little or no notice. Network and server files are backed up by Technical Services personnel, but they are not responsible for any information/files not saved to the servers.

3. Departmental rules and regulations prohibit officers from disseminating information stored on department computers. However, employees may disseminate information to authorized individuals.

4. Access rights shall be determined by assignment. Personnel requesting access to other department files/folders not associated with their current assignment, may request access through their supervisor and then must complete a Service Now request explaining the need for access and what supervisor gave the approval.

5. Personnel requesting a name change shall complete and forward a Service Now ticket to Technical Services.

6. Accounts will be disabled at the time of retirement or separation from the department.

D. LAW ENFORCEMENT DATABASES

1. Data accessed through any law enforcement database shall be restricted to the use of duly authorized law enforcement and/or criminal justice agencies for the performance of criminal justice duties. The data shall not be sold, transmitted, or disseminated to any non-law enforcement agency or unauthorized persons.

2. Personnel shall destroy all law enforcement database hard copy printouts when no longer needed.

3. MDB's with LEADS access shall not be removed from the police vehicle mount for any reason. This does not apply to Technical Services or radio 5 personnel who are acting in their official capacities of repairing or installing them.

E. EXPECTATION OF PRIVACY

1. Computer resources are owned and maintained by the Akron Police Department, which reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of computer resources, with the following exceptions:

   a. No hardware, software, or digital information that is evidence or contraband; i.e., photos depicting pornography or child pornography, will be viewed, copied, or shared in any way with anyone not directly involved with the investigation and prosecution of the case or supervisors in their direct chain of command.

   b. Computer resources used to facilitate a criminal investigation will generate information and reports that are part of the case file. No person other than assigned investigators and prosecutors, or supervisors in their direct chain of command, may copy or disseminate in any way any information, digital or otherwise, contained in a case file until that file becomes public record.

   c. Investigations conducted online may require the use of false identities and role-playing. When done in furtherance of an investigation, this is entirely appropriate and is in no way a violation of the procedure or any city policy or procedure.

2. Users understand that human or automated means may be used to monitor use of computer resources including communications, Internet access, data access, and other content transmitted, received, or stored.

F. SECURITY

1. An employee's initial network sign-on password is created by Technical Services personnel. Passwords created by Technical Service's personnel shall be immediately changed by the employee during the next log on and when prompted by the network application thereafter. Users are responsible for safeguarding their passwords and are responsible for all transactions made with their passwords.

2. No user shall allow access to their password or account by another, nor will any user use another's password or account.

3. Personnel shall not use computer resources for excessive personal use when it interferes in the performance of their job duties, consumes significant resources, interferes with the activities of other employees, or results in the waste of productive work time.

4. Personnel shall not leave work stations unattended without logging out, signing off, or locking the computer.

5. Personnel attempting to access the network using an invalid password, shall be locked out of the network after three failed log-in attempts. If this occurs, employees will be locked out of the network for 15 minutes and can try again after that time. If an employee fails to remember their password, a request to reset a password will be made by completing a Service Now ticket. If you are unable to access Service Now to enter ticket, please contact the Technical Services offices at 330-375-2216.

6. Personnel shall take reasonable steps to safeguard department issued computer equipment and all information/data contained therein.

7. Personnel shall immediately report any theft, attempted theft, or loss of department owned computer equipment, data, or passwords. Personnel shall immediately report any theft, attempted theft, or loss of any personally owned device which was enabled to access the department's network to their immediate supervisor and also to the Technical Services supervisor.

G. E-MAIL

1. Personnel having email accounts shall check their email for new messages at least once during their shift and respond accordingly.

2. Personnel shall not attempt to access another person's email. This does not apply to Technical Services personnel acting in their official capacity.

3. Personnel receiving an email with a file attachment of unknown origin, or that is not for official work purposes shall delete the entire email message without opening the attached file.

4. Personnel shall delete email messages when no longer needed or useful. All email is archived as part of the Ohio Public Records Act

5. Personnel receiving a virus alert shall contact Technical Services immediately.

6. Personnel shall not send out department-wide emails without the prior approval of their supervisor.

7. E-mail should never be considered private or secure. It may be stored indefinitely on any number of computers, including that of the recipient. Copies of messages may get forwarded to others. E-mail sent to nonexistent or incorrect user names may be delivered to persons that were never intended to receive it.

8. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate shall not be sent.

9. Chain letters are messages sent to a number of people asking each recipient to send copies to a number of other users. They consume resources and can degrade network performance or delay delivery of essential e-mail. Users should immediately delete such e-mail. If a user has received such a message that has a legitimate need to get

forwarded, it should first be evaluated for authenticity and approved by a supervisor or by the Technical Services Unit.

H. INTERNET

1. All internet traffic may be monitored and recorded by Technical Services personnel and could be made available to audit requests.

2. Material found on the internet that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate shall not be downloaded, copied or forwarded. Exceptions may be granted if the stated material is being used by the employee who is investigating criminal or civil actions.

3. Abuse of Internet privileges shall result in the loss of these privileges. In addition, the employee may be subject to disciplinary action, including possible termination, civil and criminal liabilities.

I. COMPUTER VIRUS PROTECTION

1. The end user is not required to perform any antivirus updates or scans. The updates and scans will be coordinated systematically by Technical Services personnel based on daily, weekly, and monthly needs and requirements.

2. Any employee who suspects that there may be a breach of information, computer hacking, sabotage to software or hardware, or computer virus shall immediately discontinue any further transactions and either unhook the computer from the network or leave the computer as is.

3. Notify Technical Services personnel immediately. If Technical Services personnel are not available then notify a Safety Communications supervisor.

4. Any Supervisor made aware of a possible breech shall notify Technical Services personnel immediately, including after hours.

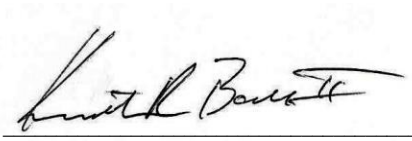
5. The Technical Services Unit supervisor will complete a LEADS Computer Incident Report Form in the event of a confirmed computer or network incident within our agency.

J. COPYRIGHTS

1. All software licensed by the City of Akron is copyright protected. It is the policy of the City of Akron not to violate copyright laws. Duplicating, selling, or otherwise copying for purposes of distributing software products, other than that which is agreed to under the terms of the software license agreement, is a violation of federal law and is forbidden by the City of Akron. The Federal Copyright Act makes no distinction between duplicating software for sale or for free distribution.

2. The rights of copyright owners will be respected. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. This includes copying text, graphics or photographs. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, it should be assumed that they are protected under copyright laws unless there is explicit permission on the materials and their use.

By Order Of,



Kenneth R. Ball II
Chief of Police

Date July 27, 2020