Louisville Metro Police Department

Standard Operating Procedures	SOP Number: 4.20
	Effective Date: 02/10/19 Revised Date: 05/29/23
	Accreditation Standards: KACP: 5.2
Chapter: Uniforms and Equipment	
Subject: Computer and Internet Usage	

4.20 COMPUTER AND INTERNET USAGE

4.20.1 DEFINITIONS

Electronic Mail (email): An electronic system for sending and receiving messages via a computer network.

Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data, including, but not limited to: mainframes, servers, personal computers, notebook computers/laptops, handheld computers/tablets, distributed processing systems, network-attached and computer-controlled medical and laboratory equipment (e.g. embedded technology), telecommunication resources, network environments, telephones and cell phones/smartphones, fax machines, printers, and service bureaus. Additionally, Information Resources are the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, governmental agencies, companies, and colleges.

Intranet: A private network for communications and sharing of information that, like the Internet, is based on transmission control protocol/internet protocol (TCP/IP), but is accessible only to authorized users within an organization.

Office of Civic Innovation and Technology (CIT): The Metro Government department responsible for computers, networking, and data management.

World Wide Web (WWW): A system of Internet hosts that supports documents formatted in Hypertext Markup Language (HTML) and contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the web with special applications called browsers, such as Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, or Google Chrome.

4.20.2 OWNERSHIP (KACP 5.2)

All information resources are owned by Metro Government and will be used in accordance with the directives outlined in the Louisville Metro Police Department's (LMPD's) Standard Operating Procedures (SOPs) and Metro Government's computer policies. Messages, files, and documents, including personal messages, files, and documents located on information resources, are owned by the department. This data may be subject to open records requests and will be accessed in accordance with this policy. Therefore, members should have no expectations of privacy in their email messages, whether sent or received, or in any other data files residing on Metro Government-owned hardware. Members should report any incidents of possible misuse or violations directly to the CIT.

In order to protect the department's interests and to verify that members are properly using information resources, the CIT may use software to monitor and log each user's activity on departmental equipment. The software restricts the use of information resources for personal benefit and may also be used to restrict access to certain programs. The use of information resources for unauthorized purposes may lead to the immediate

4.20.2 OWNERSHIP (CONTINUED)

removal of information resources access and possible disciplinary action, up to and including termination.

All files downloaded from the Internet are scanned for viruses using the current virus detection software provided by the CIT.

4.20.3 EQUIPMENT REQUIREMENTS

All computers/servers must have a CIT-approved operating system image and have the ability to be managed by the CIT.

All computers/servers connected to the network must be in compliance with the Metro Government Network Access/Configuration policy.

Members will not:

- Remove labels or change the labels placed on any equipment by the CIT.
- Move or add equipment without the approval of the CIT. This includes moving computers to another desk, printers, network equipment, etc. and installing software on Metro Government devices.
- Use external peripherals, such as Universal Serial Bus (USB) devices, that are capable of storing data, unless approved by the CIT.
- Purchase computer equipment for departmental use, without the approval of the CIT.
- Purchase or install firewalls, routers, repeaters, switches, hubs, or wireless access points, without the approval of the CIT.
- Alter network hardware, in any way.
- Use personal computers as a routing device or to extend the network.

4.20.4 COMPUTER USAGE AND RESTRICTIONS

To aid in the maintenance and security of the network, members will:

- Logoff, but leave the computer turned on, while not in use or at the end of their shift.
- Not store data on a local hard drive (C: Drive). All LMPD data is required to be stored on the network drives (U: Drive) and will be backed up by the CIT. Data is backed up, via virtual libraries and offsite storage, on a regular basis, depending on the type of information. This could be on an hourly, nightly, or weekly basis. The CIT monitors this backup to prevent needed data from being lost. Data stored on a local hard drive will not undergo network backup, and therefore, may be lost. No attempt will be made to recover data from the local hard drive.
- Not store data on active desktops. Storing data on active desktop increases logon time and, if damaged, the data may be lost. Creating shortcuts on the desktop that point to data on the network drive is recommended.

The CIT maintains a central data center and two (2) secondary data centers for high availability and disaster recovery capability.

Louisville Metro Police Department

Standard Operating Procedures	SOP Number: 4.20
	Effective Date: 02/10/19 Revised Date: 05/29/23
	Accreditation Standards: KACP: 5.2
Chapter: Uniforms and Equipment	
Subject: Computer and Internet Usage	

4.20.4 COMPUTER USAGE AND RESTRICTIONS (CONTINUED)

Members are prohibited from using information resources:

- For personal benefit or profit.
- To engage in illegal activity in violation of local, state, federal, or international law.
- To intentionally access, create, store, or transmit material which the department deems offensive, indecent, or obscene. The only permissible exception of this prohibition is for investigation purposes with the explicit approval of the division/section/unit commander.
- To engage in activities contradictory to the mission and values of the department.
- To access internet (streaming) video or audio sources or personal relationship sites/chat rooms, unless as part of an investigation or other work-related duty.
- To violate the rights of any person or company protected by copyright, patent, or other intellectual property laws; or similar laws and regulations. This includes, but is not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Metro Government.
- To create unauthorized copies of copyrighted material for which Metro Government, or the end user, does not have an active license. This includes, but is not limited to, digitization and/or distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music, or the installation of any copyrighted software.
- To provide information to parties outside of Metro Government regarding departmental members.
- To engage in an intentional breach of a local, state, or federal government information system user agreement or regulation.

As a convenience to the department-user community, incidental use of information resources is permitted. The following restrictions apply:

- Incidental use of electronic mail, Internet access, fax machines, printers, copiers, etc. is restricted to departmentally-approved users only. This does not include members' family, friends, or acquaintances.
- Incidental use that results in direct costs to the department is prohibited.
- Incidental use that interferes with the normal performance of a member's work duties is prohibited.
- No files or documents will be sent, or knowingly received, that may cause legal action against, or discredit to, the department.

Members are prohibited from putting a victim's, suspect's, or other's personally identifiable information [e.g., date of birth (DOB), Social Security Number (SSN), etc.] in the Computer Aided Dispatch (CAD) narrative from a Mobile Data Terminal (MDT) or other computer.

NCIC information may only be accessed by members with a legitimate law enforcement purpose. Due to the sensitive nature of the information, members are prohibited from copying, pasting, or otherwise entering National Crime Information Center (NCIC) information from a NCIC Terminal, MDT, or any other device into any other document, computer program, or other electronic system. However, the information may be summarized and included in case documentation. Members are also prohibited from taking photographs/screen shots of NCIC information. The NCIC will not be left visible on the screen when the computer is not in use.

Members who access the Kentucky Department of Transportation (DOT) driver's license photographs through the Mobile for Public Safety (MPS)/Informer client may use these photographs for identification purposes only.

4.20.4 COMPUTER USAGE AND RESTRICTIONS (CONTINUED)

These photographs will not be printed, copied, pasted, emailed, or otherwise entered into any other document, computer program, or other electronic system.

Members are also prohibited from taking photographs/screen shots of information obtained through the MPS/Informer client.

4.20.5 SECURITY RESTRICTIONS

Members should report any weaknesses in departmental computer security, as well as any incidents of possible misuse or violations, directly to the CIT.

Members will not violate the security of the network by:

- Actively seeking out vulnerabilities/weaknesses in the network.
- Effecting disruptions of network communication (e.g., network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information).
- Introducing malicious programs into the network (e.g., viruses, worms, Trojan horses, email bombs).
- Attempting to access another member's account.
- Attempting to access data for which they do not have authorization or explicit consent. This includes, but is not limited to, data from this department and/or any outside source. Anyone attempting unauthorized access will be considered in violation of KRS 434.853.
- Sharing accounts, passwords, personal identification numbers (PIN), or similar information or devices used for identification and authorization purposes. If a member contacts the CIT Service Desk for computer support, CIT technicians may be required to ask for a member's password in the troubleshooting process. If so, the password must be changed upon the user's next login.
- Using or installing any software (e.g. commercial, shareware, or freeware) without explicit consent from the CIT. Unauthorized software includes, but is not limited to:

    - Any software that monitors users (e.g., Spyware or Adware)
    - Peer-to-Peer software (e.g., Napster, WinMX, Kazaa, Grokster, and File Mule)
    - Instant Messaging software (e.g., AOL Instant Messenger or Yahoo Messenger)

The CIT will conduct audits, at least annually, to verify passwords and access codes, and to determine possible access violations.

4.20.6 INTERNET USAGE RESTRICTIONS

The following restrictions of Internet usage and software apply:

- Additional software for browsing the Internet or Internet tool bars (e.g., instant messages or hot bars) are prohibited, unless authorized by the CIT.
- Business-related purchases made over the Internet are subject to departmental policy.

4.20.6 INTERNET USAGE RESTRICTIONS (CONTINUED)

- Personal use of Internet access is restricted to approved departmental users and must not result in direct cost to the department.
- Internet use must not interfere with the normal performance of a member's work duties.
- No files or documents may be transmitted that may cause legal liability for, or embarrassment to, the department.
- Storage of personal files and documents within the department's information resources should be kept to a minimum.

4.20.7 EMAIL USAGE AND RESTRICTIONS

The LMPD provides technology resources for business purposes. Although members may use these resources occasionally for personal non-business purposes, such use will be in strict compliance with this policy.

Due to the limited amount of email storage space, all members must maintain their mailboxes in an appropriate manner.

Organizing email into folders and deleting unneeded email messages from the inbox and deleted items folders, makes file management easier and reduces the strain on the finite amount of storage space on departmental servers. Information contained in the system is retained pursuant to applicable records retention schedules.

Members will utilize the "Automatic Replies (Out of Office)" feature in accordance with SOP 3.4.

Departmental members will read all messages from the CIT regarding system issues (e.g., downtimes, upgrades) as they relate to the email system and other departmental applications.

Members are prohibited from:

- Using departmental email for personal gain or profit, except for approved secondary employment. Members are prohibited from sending secondary employment requests to persons or agencies outside of the LMPD, including other agencies of Louisville Metro Government.
- Sending or forwarding email to the group email distribution lists of outside businesses or agencies, including other Louisville Metro Government agencies [e.g., Louisville Metro Department of Corrections (LMDC), etc.] Exceptions may be approved and sent or forwarded by a commanding officer with the rank of lieutenant or above. Exceptions may be made for LMPD business purposes only (e.g., Wanted and/or Attempt to Locate flyers, etc.).
- Using their departmental email as an email address for personal accounts (e.g., bank accounts, eBay, etc.), unless the use has a direct relation to the member's departmental duties.
- Sending, forwarding, or storing email that is intimidating, harassing, indecent, or obscene, all as determined by the department; except to a supervisor or the CIT, for reporting purposes.
- Sending, forwarding, or storing unsolicited email messages, including the sending of "junk mail," "SPAM," or other advertising material to individuals who did not specifically request such material, except to a supervisor or the CIT, for reporting purposes.
- Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
- The unauthorized use or forging of email header information.

4.20.7 EMAIL USAGE AND RESTRICTIONS (CONTINUED)

- Soliciting email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Using a departmental email address to send or receive correspondence for a private company or business.
- Using email for the purpose of political lobbying or campaigning, except as allowed by the collective bargaining agreement with the River City Fraternal Order of Police (FOP), Lodge #614.
- Violating copyright laws by inappropriately distributing protected works.
- Emailing National Crime Information Center (NCIC) information inside or outside of the department due to its sensitive nature.
- Posing as another person, unless authorized by the division/section/unit commander, when conducting an investigation or when authorized to send messages on behalf of another, when serving in an administrative support role.
- Accessing outside personal email accounts (e.g., Hotmail, Yahoo, AOL, etc.) unless approved for investigative purposes by the Assistant Chief of Police/Administrative Bureau, or their designee.
- Sending, forwarding, or "broadcasting" messages or materials to numerous recipients without authorization from a commanding officer or professional staff supervisor. Authorization will only be granted for the following:

    - Messages with a demonstrable departmental business purpose.
    - Notifications and announcements of births, illness, deaths of members and their immediate family, or retirements of members.

- Using unauthorized email software (e.g., Pegasus, Eudora) or "plug-ins" not approved by the CIT.
- Transmitting hoaxes (e.g. "Do not use cell phones at gas pumps!" or virus warnings). If in doubt, contact the CIT, who will verify and advise users of possible hoaxes.
- Sending or forwarding excessively large messages.
- Sending or forwarding email likely to contain computer viruses.
- Attempting to bypass the file blocking of email attachments.
- Attempting to bypass system virus protection.
- Divulging their usernames or passwords, via email. Exemptions must be approved by the CIT Service Desk or the Technical Services Lieutenant. If usernames or passwords are solicited via email, members should assume that it is a scam. Members will contact the CIT Service Desk at (502) 574-4444 and advise them of suspicious solicitations. Members may report spam email by clicking on the "Phish Alert Report" button in Outlook.
- Responding to any SPAM email received via departmental email. As a large organization, Metro Government is constantly under attack by SPAM emails. These emails search for valid accounts to direct more email or security threats to. Often, these emails contain a hyperlink to remove the recipient from the SPAM email list. These hyperlinks are frequently a ploy to gain additional information on the recipient.

If an email or an email attachment contains sensitive or private information [e.g., dates of birth (DOB), Social Security Numbers (SSNs), or other personal identifying information] appropriate steps to protect that information should be taken. Users will include the phrase "[encrypt]" in the subject line so that emails containing sensitive materials will be encrypted. Personal information contained in Wanted and/or Attempt to Locate flyers sent for

4.20.7 EMAIL USAGE AND RESTRICTIONS (CONTINUED)

law enforcement purposes to other law enforcement individuals/agencies is exempt. If in doubt, contact the CIT for guidance.

4.20.8 PASSWORD SECURITY

The network will automatically prompt users to change passwords every 90 days. Users will be notified several days in advance of the expiration date. If a password is allowed to expire, the user's account will be locked, and the user will need to call the CIT Service Desk at (502) 574-4444 to reactivate their account.

Passwords of at least nine (9) characters will be constructed, with at least three (3) of the following embedded:

- English upper-case characters (e.g. A-Z)
- English lower-case characters (e.g. a-z)
- Digits (e.g. 0-9)
- Non-alphabetic characters (e.g. @#$%^&*()_+)

When constructing a password, the following are not recommended:

- User's account name or parts of the user's full name that exceed two (2) consecutive characters
- Words found in English or foreign dictionaries
- Slang, dialect, jargon, etc.
- Previously-used passwords
- Names of family members, pets, friends, coworkers, etc.
- Computer terms and names, commands, sites, companies, hardware, or software
- Personal information (e.g., birthdays, addresses, phone numbers)
- Letter or number patterns (e.g., aaabbb, qwerty, 123321)
- Any of the above preceded or followed by a digit (e.g., 1secret, secret1)

Passwords are to be kept secure and confidential. Any suspected loss of password information must be immediately brought to the attention of the Technical Services Lieutenant so that a new password may be issued. If passwords and/or access codes do not meet these requirements, the user's account may be disabled.

4.20.9 PASSWORD RESTRICTIONS

Password users will be held accountable for all actions taken with their account. Workstations must be secured anytime the computer is left unattended. Employees must logoff, lock the computer, or activate a password-protected screen saver each time the workstation is left unattended. The use of the screen saver idle time lock activation is mandatory.

All passwords are to be considered confidential departmental information. To maintain password security, users will not:

- Use the same password for departmental accounts as for personal accounts (e.g. ISP accounts, web

4.20.9 PASSWORD RESTRICTIONS

mail, financial institutions).
- Reveal a password in an email, over the telephone, on questionnaires, or on security forms.
- Reveal a password to supervisors, family members, coworkers, or others.

4.20.10 CONTRACTUAL EMPLOYEES, UNPAID INTERNS, AND VOLUNTEERS

It is the responsibility of the commanding officer of the contractual employee, unpaid intern, or volunteer to notify the CIT Service Desk at (502) 574-4444 upon the contractual employee, unpaid intern, or volunteer's departure from the department, so that their computer account can be disabled.

4.20.11 INTRANET

The LMPD maintains a departmental Intranet homepage ("blue page"), which is accessible to members via a departmental computer.

Through this homepage, members are able to access links to various resources including, but not limited to, the following:

- TeleStaff
- BlueTeam
- EIPro
- Courtnet
- Evidence.com
- eWarrants
- Forms
- JusticeXchange
- Kentucky Revised Statutes (KRS)
- Louisville Metro Code of Ordinances (LMCO)
- Kentucky Sex Offender Registry
- LMPD SOPs
- Workday
- Kentucky Open Portal Solution (KYOPS)
- PowerDMS