

**Policy:**

All computer resources are the property of Lee County and are intended to be used for approved County business purposes. Users are permitted access to the computer system to assist them in the performance of their jobs. Limited personal use of the computer system is permitted when the use does not (1) interfere with the user's work performance; (2) interfere with any other user's work performance; (3) have undue impact on the operation of the computer system; or (4) violate any other provision of this policy or any other policy, guideline, or standard of Lee County. At all times, users have the responsibility to use computer resources in a professional, ethical, and lawful manner. Personal use of the computer system is a privilege that may be monitored, restricted or revoked at any time.

**204:1 No Expectation of Privacy**

1. *No Expectation of Privacy.* The computers and computer accounts given to users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the Board of County Commissioners and is intended for business purposes. A computer's hardware content may be deleted and/or cleaned with the approval of the Department Director and in accordance with Chapter 119, Florida Statutes.
2. *Waiver of Privacy Rights.* Users expressly waive any right of privacy in anything they create, store, send, or receive on the County's computers or computer network, or on County-issued electronic devices. Users consent to allowing personnel of the County to access and review all such materials. Users understand that Lee County Government may use human or automated means to monitor use of its computer resources.
3. *Public Records.* Generally, documents that are created to formalize knowledge or transact business of the County are considered public records open to the review and copying of the general public. This includes, but is not limited to, all such records created, stored, sent, or received on the County computer system, and created, stored, sent or received on a cell phone or similar personal electronic device, whether the device belongs to the employee or is issued by the County. Records of e-mail messages, text messages, and records of inbound and outbound calls must be retained in accordance with the provisions of Chapter 119, Florida Statutes. Do not delete a public record! If you have any question whether a particular item is a public record, please consult the Human Resources Department.
  - Since Chapter 119, Florida Statutes states that all documents/work product made or received in connection with the transaction of official County business are to be considered public records, any County related work done on a computer at home or away from County facilities must be saved to disk, transferred to the employee's office computer, or produced in another media where the public may have access (e.g., on paper).

**204:2 Prohibited Activities**

Violations of any portion of this policy may be subject to disciplinary action up to and including termination of employment.

1. *Inappropriate or Unlawful Material.* Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or

## COMPUTER RESOURCES

Policy Number 204

Page 2 of 6



inappropriate may not be sent by email or other form of electronic communication or displayed on or stored in the County's computers, including, but not limited to, messages and material with sexual comments, obscenities, pornography, abusive or degrading language, antisocial behavior, or inappropriate comments concerning race, color, religion, sex, national origin, marital status, or disability. Users encountering or receiving this kind of material must immediately report the incident to their supervisors. Violations of this policy may result in disciplinary action, including discharge. If the employee is receiving inappropriate email, as described, from their supervisor or management personnel it must be reported to Human Resources.

2. *Prohibited Uses.* Lee County's computer resources may not be used for dissemination or storage of commercial or personal advertisements or solicitations, promotions, destructive programs (that is viruses or self-replicating code), political material, or any unauthorized use deemed inappropriate by the County.
3. *Social Media.* Without prior written permission from the County, users may not use instant messaging, text messaging, social networking sites, including but not limited to Twitter, Facebook, MySpace Linked In, for any official County communication. Please see the Manual's social media policy for additional guidance.
4. *Waste of Computer Resources.* Users may not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, sending and/or receiving personal (non-business) instant messages, printing multiple copies of documents, using hard drive or network space to store personal data, or creating unnecessary network traffic.
5. *Misuse of Software.* Most of the software used by Lee County is licensed with a limitation that it may be used by Lee County employees. It should not be treated as "shareware" even with consultants and/or other government employees. Without prior written authorization from the County, users may not do any of the following: (1) copy third party software for use on their home computers; (2) provide copies of third party software to any independent contractor, client, or third person; (3) install any software on Lee County's workstations or servers; (4) download any software from the Internet or other online service to any Lee County workstation or server; (5) modify, revise, transform, recast, or adapt any software; or (6) reverse-engineer, disassemble, or decompile any software. Violations of this policy may result in disciplinary action, including discharge, and possible civil and/or criminal penalties. Employees who become aware of any misuse of software or violation of copyright law must immediately report the incident to the Director of Human Resources.
6. *Disguising Identity.* Users must not alter the attribution-of-origin information, or "From:" line, in e-mail messages or postings. Anonymous or pseudonymous electronic communications are forbidden. (Users may not, under any circumstances, use "spoofing" or other means to disguise their identity in sending e-mail.)
7. *Personal Computer Modifications.* Users may not attempt to repair personal computers and peripherals when the repairs involve changing or replacing internal component parts. Users may not make changes that affect the personal computer setup, network settings, or overall operation. Users are authorized to change consumables such as toner cartridges, ribbons, paper, etc.

**Adopted by the Lee County BoCC May 11, 1994 (Last Revised June 20, 2017)**

**204:3 Passwords**

1. *Responsibility for Passwords.* Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords may not be printed, stored online, or given to others. Users are responsible for all transactions made using their User Identification. No user may access the computer system with another user's password or account. Violations of this policy are subject to discipline up to and including discharge.
2. *Passwords Do Not Imply Privacy.* Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that users have an expectation of privacy in the material they create or receive on the computer system. Lee County has global passwords that permit access to all material stored on its computer system – regardless of whether that material has been encoded with a particular user's password.
3. The Information Technology Group (ITG) can reset any and/or all passwords with a Director's permission if needed. Password lists are not allowed.

**204:4 Security**

1. *Accessing Other User's Files.* Users may not alter or copy a file belonging to another user without first obtaining permission from the creator of the file. Ability to read, alter, or copy a file created by another does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other users by unnecessarily reviewing their files or e-mail.
2. *Accessing Other Computers & Networks.* A user's ability to connect to other computer systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.
3. *Computer Security.* Each user is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of Lee County's computer resources. This duty includes taking reasonable precautions to prevent intruders from accessing the County's network without authorization and to prevent introduction and spread of viruses.
4. *Remote Access.* Employees may only access data for which they have been authorized. Employees may not share access methodologies and/or access with others.

**204:5 Viruses**

1. *Virus Detection.* Viruses can cause substantial damage to computer systems. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses to the County's network. To that end, all material received on floppy or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to Lee County **MUST** be scanned for viruses and other destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops might contain viruses. All disks transferred from these computers to the County's network **MUST** be scanned for viruses.

## COMPUTER RESOURCES

Policy Number 204

Page 4 of 6



2. *Accessing the Internet.* To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to the County's network must do so through an approved Internet firewall. Accessing the Internet directly, when connected to the County network (ex: by modem), is strictly prohibited.

### 204:6 Encryption Software

1. *Use of Encryption Software.* Users may not install or use encryption software on any of the County's computers without an appropriate business justification and written permission from their supervisors and the Information Technology Group. Approved users may not use encryption keys that are unknown to their supervisors.
2. *Export Restrictions.* The Federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States without prior written authorization from the County Manager and County Attorney.

### 204:7 Home Use of County Computers

1. Supervisors have the discretion to allow Lee County computers to be used by employees at home for County-related work purposes, including telecommuting work arrangements (See Alternative Work Arrangements Policy 209).
2. The employee requesting use of a computer at home and his or her supervisor must sign an "Agreement for County Computer Use at Home" which should be developed by each department.
3. The employee agrees to abide by all provisions of the County policy while using the County computer at home. The employee shall not use the computer for personal use requiring any storage of data to the hard disk or loading of software or applications. Nor shall the personal use of the computer violate the provisions of this or any County policy.

### 204:8 Additional Provisions

1. *Disclaimer of Liability for the Use of the Internet.* Lee County is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of those pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.
2. *Compliance with Applicable Laws and Licenses.* In their use of computer resources, users must comply with all software licenses; copyrights; and all other state, federal, and international laws governing intellectual property and online activities.

3. *E-mail Signature.* Users must sign all e-mail and all other electronic correspondence in accordance with the protocol established:

Full Name  
Title & Department  
E-mail address ([id@leegov.com](mailto:id@leegov.com))  
Phone Number  
FAX Number

4. *Permanency of E-mail.* Employees are encouraged to give careful thought and consideration to what is communicated via e-mail (especially externally). Do not send an e-mail that would differ in content or expression from a formal memorandum. Email archiving is done automatically for users.
5. *Ownership Rights.* All computer hardware, software, peripherals, disks, and data purchased by the County, created for use by the County, or created in the execution of County business, are the sole property of the Lee County Board of County Commissioners.
6. *Amendments, Revisions & Unspecified Aspects of Policy.* Any interpretation of this policy as it relates to the computer system will be provided by the Department of Human Resources with guidance from ITG and the County Attorney's Office.

### **204:9 Computing Environment**

1. *Software/Hardware Procurement.* All software and hardware must be obtained (free software, grant, normal purchase, etc.) through existing purchasing procedures.
2. *Software and Hardware Installation.* All software must be installed by ITG. Any personal or test software/hardware installed by any individual may be removed from the computer resource at any time. There should be no expectation for non-approved software/hardware to remain in the computer resource after maintenance, upgrades or replacement.

## COMPUTER RESOURCES

Policy Number 204

Page 6 of 6



*This page intentionally left blank*