iPad 1:1
PACE Initiative

CHAPTER 1

iPad Handbook

Auburn City Schools is excited to offer students in grades 7 – 12 an iPad to use at school and at home. The 1:1 iPad Program will enhance the delivery and individualization of instruction. Learning results from continuous dynamic interaction among students, educators, parents, and the extended community. Effective teaching and learning with iPads integrates technology into the curriculum anytime, anywhere.

Specifications

iPad

- 128 GB
- 9.7-inch diagonal LED-backlit Multi-Touch display with IPS technology
- A10 Fusion Chip with 64-bit architecture
- Embedded M10 coprocessor
- 10 watt power adapter
- Lightening to USB cable

Rugged Combo 2 Case

- Detachable keyboard
- Adjustable stand

SECTION 1

Vision

ACS will infuse information and communication technologies as well as digital learning resources into a vibrant learning community that promotes inquiry, analysis, and creativity as a catalyst for positive universal impact.

SECTION 2

Expectations

For students and parents/guardians, the following information is provided to help everyone understand the expectations and the responsibility of care and use related to receiving an iPad:

- Students will receive instruction from school staff on the proper use of the iPad.
- Students will be able to take the iPad home during the school year.
- Students are to remain in possession of their iPad at all times.
- Students are expected to treat the iPad as a valuable piece of equipment.
- Students must take all precautions to prevent theft; for example, do not leave the iPad unattended or in the passenger area of a car.
- Students must take precautions to prevent damage to the iPad; for example do not leave the iPad where there is danger of coming in contact with moisture or excessive heat. This would include protecting the iPad from inclement weather.
- The iPad comes with preloaded apps that must not be removed. Students may only load additional apps and resources from self-service.
- Students are to use the iPad to access only educationally and socially appropriate materials and websites.
- Students must not use the iPad to purchase goods and services via the Internet. (Parents/students are responsible for any financial obligations incurred from the inappropriate use of the iPad.)
- Students are to use the iPad in accordance with the Auburn City Schools' *Technology Use and Guidelines* policy and to maintain the iPad in accordance with the procedures and information provided.
- Students are expected to adhere to any additional requirements set forth by the classroom teacher.
- iPads are the property of Auburn City Schools and must be returned at the end of the academic year, upon withdrawal from Auburn City Schools, or at the request of a teacher or administrator. Willful failure to return the iPad in accor-

dance with the stated conditions will result in criminal prosecution.

- Since the iPads are the property of Auburn City Schools, officials of the school have the right to review all material stored on or accessed by any iPad.
- School officials may revoke a student's iPad use privileges for misuse or violation of policies.

SECTION 3

Technology Use and Guidelines Policy

Privacy Notice and Notification of Technology

The District's computer technology, network, and Internet System are to be used for educational and professional purposes. Users are reminded that all computer, network, and Internet use may be monitored by the District, and that there is no assurance of privacy or warranty of any kind, either expressed or implied, or that all services provided through this system will be error free or without defect. All users of this system agree to abide by all district policies, and guideline rules as written in this document.

Notification of Blocking, Filtering, and Monitoring of Technology

The *Electronic Communications Privacy Act of 1986* allows for schools to utilize a blocking/filtering system where it relates to review of communications once they are stored in a school or district system, monitoring for legitimate purposes where one (1) party has previously consented to such monitoring (Acceptable Use Agreement), and monitoring by personnel performing duties necessary to maintaining the computer systems or to protecting the rights or property of Auburn City Schools.

The *Children's Internet Protection Act* (PL 106-554) requires that schools implement technology measures to protect minors from visual depictions that are obscene, pornographic, or "harmful to minors." Students and staff of ACS are subject to the provisions of the *Alabama Digital Crime Act* (2012).

Controversial Material

Users may encounter material which is controversial and which users, parent, teachers, or administrators may consider inappropriate or offensive. It is the users' responsibility not to initiate access to such material. Users who voluntarily access such material may be prohibited from using the Internet.

Audio And/Or Video Recording Devices Procedures

Recordings may not be used to capture confidential student information protected by the *Family Educational Rights and Privacy Act* (FERPA) and copyrighted materials protected under federal law.

These procedures regulate the use of any device that records audio or video in the school environment, particularly the classroom. All students and visitors must adhere to the following:

1. Students may possess instructional technology devices that record audio and/or video and utilize them as instructional tools in the classroom only with the consent and under the direction of the school administration and teacher, as it pertains to the curricular unit, lesson or assignment.

2. Except in the circumstances of an observation with prior written authorization by the Principal pursuant to the district's Formal Classroom Observation Procedures, all active recordings must be disclosed prior to recording to all parties present during recording. Parents/guardians are permitted to make an audio recording of an Individualized Education Program (IEP) meeting in accordance with this procedure, as long as the intent to record the meeting is disclosed prior to the meeting in order to allow the District the opportunity to record the meeting as well.

3. Hidden recording devices are not permissible.

4. All recording devices must be powered off when not in use.

5. Publication of recording without prior written notice to and consent from the Principal is prohibited.

6. Recording of private conversations without agreement by all parties is strictly prohibited.

7. All recordings must be in compliance with state and/or federal recording and/or wiretapping laws. All copyright and intellectual property laws and restrictions apply.

8. If a meeting (including an IEP meeting) is being audio recorded, the school will not keep a written conference record of the meeting as a more detailed documentation is being developed through the use of audio recording.

Acceptable Use of Technology Equipment

Students attending Auburn City Schools (hereinafter referred to as ACS) are encouraged to utilize the computing capability of ACS in pursuit of their educational objectives. ACS strives to keep up-to-date equipment, software, and communications capabilities at all schools in the system. Students and their parents/guardians in return for the privilege of using the computing resources, software, and communication infrastructure of ACS must agree to this policy. Students and their parents agree that violation of these policies could result in the suspension of their privilege of using the ACS computing resources, but will not relieve or waive the responsibility of the students to complete any work assigned by their teachers.

The use of computers at Auburn City Schools is a privilege afforded to our students to enrich their education and prepare them for the technology they will use in both college and the workforce after graduation. Students who abuse this privilege in any way will be barred from using the computers in the future and subject to discipline appropriate for the offense. Disciplinary measures can include the following: detention hall, ISS, out-of-school suspension, expulsion, and/or legal charges if in violation of state and federal law.

Proper and Ethical Use

With this learning tool, students and staff must understand and practice proper and ethical use. All individuals using this system must attend in-service training (or receive special instructions) regarding procedures, ethics and security involving using the Internet.

*For additional information on the use of school iPads at Auburn Jr. High, Auburn High School, and East Samford School refer to the "Student/Parent iPad Agreement" provided at the school.

No Student or Staff Personnel Shall:

1. Utilize ACS computing resources except for the purpose of meeting educational requirements of an activity directly assigned as part of classroom work, extra credit activity, or school–supported functions, which are supervised and monitored by school personnel. Students are to use the computers only for educational purposes related to their classes. Things they may not use the computers for include but are not limited to, games, chat rooms, downloading any type of music, movies, videos, pictures, etc. E–mail is to be used only when supervised by a teacher for educational activities. Students are not to use the internet to access any type of pornographic sites, sites containing profanity, or other sites inappropriate for the educational setting. At no time will a secondary (grades 6–12) student be allowed to use a faculty member's computer for any reason.

2. Access, transmit, copy, or retransmit material, which promotes violence or destruction of property or the manufacture and use of explosive or destructive devices such as, but not limited to, explosives, fireworks incendiary devices or other devices capable of causing injury or damage to property.

3. Access, transmit, copy, or retransmit any material judged obscene by community standards as defined by the Auburn City Board of Education or any entity designated by the Board to provide such definition.
Material, including text, lyrics, images, or sound that is pornographic material designed to stimulate erotic feelings by the description or portrayal of sexual activity, is strictly prohibited.

4. Access, transmit, copy or retransmit material which promotes or advocates violence, hatred, harassment, defamation, cyber bullying or discrimination against any individual or group on the basis of race, ethnic origin, gender, age, religion, sexual preference and/or disability.

5. Utilize ACS computer resources to purchase, lease, sell, or otherwise engage in any form of commerce.

6. Access, transmit, copy, create, possess, or retransmit software, executable files, codes, scripts, macros, or any other material not specifically authorized and installed by ACS.

7. Commit or attempt to commit any willful act involving the use of ACS equipment or network capabilities that disrupt the operation of the ACS equipment or network capabilities.

8. Access, transmit, copy, create, possess, or retransmit software, executable files, code, scripts, macros, or any other material commonly known as a computer virus or worm.

9. Access, create, engage in or otherwise participate in role–playing or the playing of games or gaming software, other than as specially authorized by ACS personnel.

10. Willfully or negligently, damage ACS equipment or facilities including but not limited to computing equipment, network equipment, printers, or other peripheral equipment.

11. Hold over reimbursement to ACS for the cost of repair to pre-damage status or value of the equipment as determined by ACS including labor at the prevailing local rate for any willful or negligent damage.

12. Copy, retrieve, modify, transmit, or retransmit copyrighted materials, except with permission, or as a single copy to reference only.

Network Etiquette

- Be polite. Do not use abusive or otherwise inappropriate language in your communications.
- Do not reveal physical addresses of students or colleagues unless approved by those individuals. E–mail addresses are frequently shared and may be used.
- Do not use the network in such a way that you would disrupt the use of the network by others.
- All users have the same right to use equipment. Users shall not play games, or use the computer resources for other non–academic activities when other users require the system for academic purposes.

This information was taken from the ACS Parent and Student Handbook beginning on page 41.

SECTION 4

Student/Parent iPad Agreement

Auburn City Schools

Student/Parent iPad Agreement

2019-2020

- I will use my iPad in ways that are appropriate, meet Auburn City Schools expectations and are educational.
- I will use appropriate language when using e-mails, journals, wikis, blogs, or other forms of communication.
- I will not create, or encourage others to create, discourteous or abusive content.
- I will not use electronic communication to spread rumors, gossip or engage in activity that is harmful to other persons.
- I understand that my iPad is subject to inspection at any time without notice and remains the property of Auburn City Schools.
- I will follow the policies outlined in the *iPad Handbook* and the *Technology Use and Guidelines* while at school, as well as outside the school day.
- I will take proper care of my iPad.
- I will never leave my iPad unattended.
- I will never loan out my iPad to other individuals.
- I will know where my iPad is at all times.
- I will charge my iPad's battery daily and arrive at school with my device charged.
- I will keep food and beverages away from my iPad since they may cause damage to the device.
- I will not use the iPad camera to take and/or distribute inappropriate or unethical material.
- I will not disassemble any part of my iPad or attempt any repairs.
- I will protect my iPad by only carrying it while in the case provided. I will not remove my iPad from the case provided by Auburn City Schools. I will keep the keyboard attached to the case.

- I will not place decorations (such as stickers, markers, etc.) on my iPad or provided case.
- I will not deface the fixed asset tag on any iPad.
- I will file a police report in case of theft, vandalism, and other acts covered by insurance as well as report to the administration of Auburn City Schools.
- I will be responsible for all damages or loss caused by neglect or abuse.

I agree to return the iPad, case, keyboard, power adapter, and USB cable in good working condition. I agree to the stipulations set forth in the *iPad Handbook*, *Technology Use and Guidelines*, and the *Student/Parent iPad Agreement*.

Student First and Last Name (Please Print)_____

Student Signature _____ Date: _____

Parent/Guardian First and Last Name (Please Print)_____

Parent/Guardian Signature _____ Date: _____

Individual school iPads must be returned to Auburn City Schools at the end of each school year.

Students who withdraw, are suspended or expelled, or terminate enrollment at Auburn City Schools for any reason must return their individual school iPad and accessories on the date of termination.

NOTE: An iPad will not be issued until the Student/Parent iPad Agreement is signed and $50 Technology Fee is received.

Terms of the Student/Parent iPad Agreement

Non-refundable Technology User Fees of $50, annually, must be paid prior to taking possession of the property. You will comply at all times with the Auburn City Schools district's *Student/Parent iPad Agreement* and *Technology Use and Guidelines Policy*. Any failure to comply ends your right of possession effective immediately.

If this fee creates a financial hardship on the student or parent from obtaining a iPad, please contact the school administration about payment options. Upon proof of financial hardship, the administration may elect to create a payment plan for the student to pay out fees over time.

Title

Legal title to the property is with the district and shall at all times remain in the district. Your right of possession and use

is limited to and conditioned on your full and complete compliance with the *Student/Parent iPad Agreement*. The student in whose name a system account and/or iPad are issued will be responsible at all times for its appropriate care and use.

Liability

The permission granted to the student ceases on the last calendar day for the current school year (unless terminated earlier by ACS). Failure to return the said iPad on or before this date to the campus Principal or his/her designee may result in criminal charges being sought against the student and/or the person who has the iPad. Auburn City Schools reserves the right at any time to demand return of the iPad forthwith.

Off-Campus Incidents

In case of theft, vandalism, or other criminal acts that occur off-campus, students must report the incident to the school no later than the next school day. A police report MUST be filed by the student or parent within 48 hours of the occurrence. A copy of the police report must be provided to the school. Upon receipt of the police report validating theft, vandalism or other criminal act, the student will not be charged for the cost of the unit.

On-Campus Incidents

On-campus incidents must be reported to ACS Administration or designee. A police report will be filed as needed.

Fair Market Value Chart (FMV)

Students will be charged the Fair Market Value for stolen, damaged, or vandalized iPads that are not reported to the police (see Fair Market Value Chart). The original cost to the district for each iPad was $535.

FAIR MARKET VALUE CHART AGE OF IPAD | VALUE	
1 Year or Less	85% of FMV
2 Years	70% of FMV
3 Years	55% of FMV
4 Years	40% of FMV

Accidental Damage

Students/Parents are responsible for repair costs of iPads that are accidentally damaged (see Damage and Neglect chart below).

The costs of any other parts needed for repairs will be based on manufacturer's current price list.

DAMAGE AND NEGLECT	
Broken Screen	$200
Apple 12W USB Power Adapter	$16
Lightning to USB Cable	$12
Rugged Combo Case and Keyboard	$100
Keyboard	$50
Re-format due to violation of *Technology Use and Guidelines* policy	$15

Repossession

If a student does not timely and fully comply with all terms of this agreement and the *Student/Parent iPad Agreement*, ACS has the right to notify the authorities to come to the student's place of residence to pick up the property.

SECTION 5

Receiving and Returning Your iPad

Receiving Your iPad

Distribution of iPads will occur at the beginning of the school year. Before receiving an iPad, students and parents must pay the $50 Technology Use Fee and sign the following online forms:

- *Student/Parent iPad Agreement*
- *Technology Use and Guidelines*, acknowledged in online registration

Any student that needs assistance with the Technology Use Fee should contact administration.

Returning Your iPad

- iPads along with the case and keyboard will be returned during the final week of school.
    - **NOTE** - Students will **keep** the power adapter and USB cable until they graduate or withdraw from school.
    - ACS will provide the first power adapter and USB cable. Students are responsible for purchasing replacement chargers.
- If a student withdraws or transfers out of the Auburn City Schools District during the school year, their iPad will be returned at that time.
- Students who withdraw, are suspended or expelled, or terminate enrollment at Auburn City Schools for any other reason must return their iPad, case, keyboard, and Apple adapter and USB cable, on the date of termination.
- The student must return the iPad, case, and keyboard in satisfactory condition and will be responsible for any damage to the iPad and/or accessories. The student will be charged a fee for any needed repairs, not to exceed the replacement cost of the iPad.
- If a student fails to return the iPad at the end of the school year or upon termination of enrollment, that student will be subject to criminal prosecution or civil liability. The student will also pay the cost of the iPad. Failure to return the iPad will result in a theft report being filed with the Auburn Police Department.

SECTION 6

Taking Care of Your iPad

Students are responsible for the general care of the iPad they have been issued by the school. iPads that are broken or fail to work properly must be taken to the iPad Help Center for an evaluation of the equipment.

Students must maintain possession of their iPads at all times.

General Precautions

- The iPad is the property of Auburn City Schools and all users will follow this policy and the *Technology Use and Guidelines* policy.
- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Cords and cables must be inserted carefully into the iPad to prevent damage.
- iPad and case must remain free of any writing, drawing, stickers, or labels that are not the property of Auburn City Schools.
- iPads must never be left in an unattended or unsupervised area.
- Students are responsible for keeping their iPad's battery charged for school each day.
- Students must keep their iPad in the protective case, provided by the school, at all times.
- Students are NOT to remove the iPad from the case. Visit the Help Center if you suspect problems with the case.
- Students must keep the keyboard attached to the case.

Carrying iPads

The protective case with attached keyboard provides the iPad with sufficient padding to protect the iPad from normal treatment and provides a suitable means for carrying the device within the school. The guidelines below should be followed:

- iPads must always be within the protective case and have the keyboard attached.
- Limit the number of items carried within a backpack with the iPad to limit the amount of pressure applied to the iPad screen.
- Avoid bumping the iPad against any surface.

Screen Care

The iPad screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the iPad at any time.
- Do not place anything near the iPad that could put pressure on the screen
- Do not place anything in your backpack that will press against the screen.
- Clean the screen with a soft, dry cloth or anti-static cloth. Use of harsh chemicals WILL damage the screen.
- Do not "bump" the iPad against lockers, walls, car doors, floors, etc. as it will eventually break the screen.

No Loaning or Borrowing iPads

- Do not loan iPads to other students or non-students.
- Do not borrow an iPad from another student or non-student.
- Do not share passcodes, passwords, or usernames.

Unauthorized Access or Hacking

Access to another person's account or device/computer without his/her consent or knowledge is considered hacking and is in violation of Section 13A-8-103 [Alabama Computer Crime Act].

SECTION 7

Using Your iPad at School

iPads are intended for use at school each day. In addition to teacher expectations for iPad use, school messages, announcements, calendars and schedules may be accessed using the iPad. Students must be responsible to bring their iPad to all classes, unless specifically instructed not to do so by their teacher. The iPad is the property of Auburn City Schools; therefore, school staff and administration have the right to check any material stored on a student's iPad at any time.

iPads Left at Home

If students leave their iPad at home, they are responsible for getting the course work completed as if they had their iPads present.

iPad Undergoing Repair

Loaner iPads may be issued to students when they leave their iPads for repair in the iPad Help Center. There may be a delay in getting an iPad should the school not have enough to loan.

Charging Your iPad's Battery

iPads must be brought to school each day in a fully charged condition. Students need to charge their iPads each evening. Only charge your iPad with the provided charger.

Sound, Music, Games, and Apps

Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.

Music is allowed on the iPad and can be used at the discretion of the teacher.

Games (web-based or apps) are not allowed on the iPad.

Printing at School

Printing will not be available from the iPad. If students need to print a file they will need to email the document to themselves or save to OneDrive in Office 365 and then print from designated computers.

Home Internet Access

Students are allowed to set up wireless networks on the iPads. This will assist them with iPad use while at home.

Printing from the iPad is an option when using a printer with AirPrint capability.

SECTION 8

Managing Your Files

Saving Your Work

Students may save work on the iPad on a limited basis. It is ***strongly recommended*** that students store files in Office 365 using the OneDrive app. Storage space will be available on the iPad – but it will not be backed up. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. iPad malfunctions are not an acceptable excuse for not submitting work.

Network Connectivity

Auburn City Schools makes no guarantee that the network will be up and running 100% of the time. In the rare case that the network is down, the district will not be responsible for lost or missing data.

Use of iPads on the Network

Auburn City Schools is committed to the importance of a student being able to continue working on assignments when an iPad is experiencing problems. To assist with this problem the district is providing the following:

Office 365

Student logins will provide access to Office 365 which can be accessed anywhere with an Internet connection. Students can save important files in Office 365 and OneDrive.

iPad Undergoing Repair

Loaner iPads may be issued to students when they leave their iPads for repair in the iPad Help Center. There may be a delay in getting an iPad should the school not have enough to loan.

Internet Resources

Online assignments may be posted through Internet resources using Schoology or classroom web pages. Talk with your student's teachers about the availability of coursework and assignments.

SECTION 9

iPad Apps

Originally Installed Software/Apps

The software/apps originally installed by Auburn City Schools must remain on the iPad in usable condition and be easily accessible at all times. From time to time additional software/apps may be added for use in a particular course.

Apps

Students are only allowed to install/download apps available in Self Service.

Inspection

Students may be selected at random to provide the iPad for inspection. These inspections may include an inspection of all material saved on the iPad.

Procedure for Re-Formatting the iPad

If technical difficulties occur that require the iPad to be restored to its original state, ACS does not accept responsibility for the loss of any software or documents deleted due to a re-format.

If technical difficulties occur that are the result of illegal software or non-Auburn City Schools-installed apps are discovered, the iPad will be restored to its original state. The school does not accept responsibility for the loss of any software or documents deleted due to a re-format. A $15 reformatting fee will be required per incident.

Software Upgrades

Upgraded versions of licensed software/apps are available from time to time. Students will be required to check in their iPads for periodic updates and syncing.

Article 5A The Alabama Digital Crime Act

Section 13A-8-110

Short title.

This article may be cited as The Alabama Digital Crime Act.

(Act 2012-432, p. 1192, §1.)

Section 13A-8-111

Definitions.

As used in this article, the following terms shall have the following meanings:

(1) ACCESS. To gain entry to, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer system, or computer network.

(2) COMPUTER. An electronic, magnetic, optical, electrochemical, or other high speed data processing device or system that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(3) COMPUTER NETWORK. The interconnection of two or more computers or computer systems that transmit data over communication circuits connecting them.

(4) COMPUTER PROGRAM. An ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(5) COMPUTER SECURITY SYSTEM. The design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.

(6) COMPUTER SERVICES. The product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(7) COMPUTER SOFTWARE. A set of instructions or statements, and related data, that when executed in actual or modi-

fied form, cause a computer, computer system, or computer network to perform specific functions.

(8) COMPUTER SYSTEM. A set of related or interconnected computer or computer network equipment, devices and software.

(9) DATA. A representation of information, knowledge, facts, concepts, or instructions, which are prepared and are intended for use in a computer, computer system, or computer network. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit.

(10) ELECTRONIC MAIL MESSAGE. A message sent to a unique destination that consists of a unique user name or mailbox and a reference to an Internet domain, whether or not displayed, to which such message can be sent or delivered.

(11) EXCEEDS AUTHORIZATION OF USE. Accessing a computer, computer network, or other digital device with actual or perceived authorization, and using such access to obtain or alter information that the accessor is not entitled to obtain or alter.

(12) FINANCIAL INSTRUMENT. Includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(13) HARM. Partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(14) IDENTIFICATION DOCUMENT. Any document containing data that is issued to an individual and which that individual, and only that individual, uses alone or in conjunction with any other information for the primary purpose of establishing his or her identity or accessing his or her financial information or benefits. Identification documents specifically include, but are not limited to, the following:

a. Government issued driver's licenses or identification cards.

b. Payment cards such as credit cards, debit cards, and ATM cards.

c. Passports.

d. Health insurance or benefit cards.

e. Identification cards issued by educational institutions.

f. Identification cards for employees or contractors.

g. Benefit cards issued in conjunction with any government supported aid program.

h. Library cards issued by any public library.

(15) IDENTIFYING INFORMATION. Specific details that can be used to access a person's financial accounts, obtain identifi-

cation, or to obtain goods or services, including, but not limited to:

a. Social Security number.

b. Driver's license number.

c. Bank account number.

d. Credit card or debit card number.

e. Personal identification number (PIN).

f. Automated or electronic signature.

g. Unique biometric data.

h. Account password.

(16) INTEGRATED CIRCUIT CARD. Also known as a smart card or chip card, a pocket sized, plastic card with embedded integrated circuits used for data storage or special purpose processing used to validate personal identification numbers (PINs), authorize purchases, verify account balances and store personal records. When inserted into a reader, it transfers data to and from a central computer.

(17) OWNER. An owner or lessee of a computer or a computer network, or an owner, lessee, or licensee of computer data, computer programs, or computer software.

(18) PROPERTY. Includes a financial instrument, data, databases, data while in transit, computer software, computer programs, documents associated with computer systems and computer programs, or copies whether tangible or intangible.

(19) RADIO FREQUENCY IDENTIFICATION (RFID). A technology that uses radio waves to transmit data remotely from an RFID tag, through a reader, from identification documents. It is used in contactless integrated circuit cards, also known as proximity cards.

(20) RADIO FREQUENCY IDENTIFICATION (RFID) TAGS. Also known as RFID labels, the hardware for an RFID system that electronically stores and processes information, and receives and transmits the signal.

(21) REENCODER. An electronic device that places encoded information from the magnetic strip, integrated circuit, RFID tag of an identification document onto the magnetic strip, integrated circuit, or RFID tag of a different identification document.

(22) SCANNING DEVICE. A scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip, integrated circuit, or RFID tag of an identification document.

(23) VIRUS. Means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted pro-

gram or other set of instructions to one or more computer programs or files.

(24) WEB PAGE. A location that has a single uniform resource locator or other single location with respect to the Internet.

(Act 2012-432, p. 1192, §2.)

Section 13A-8-112

Computer tampering.

(a) A person who acts without authority or who exceeds authorization of use commits the crime of computer tampering by knowingly:

(1) Accessing and altering, damaging, or destroying any computer, computer system, or computer network.

(2) Altering, damaging, deleting, or destroying computer programs or data.

(3) Disclosing, using, controlling, or taking computer programs, data, or supporting documentation residing in, or existing internal or external to, a computer, computer system, or network.

(4) Directly or indirectly introducing a computer contaminator or a virus into any computer, computer system, or network.

(5) Disrupting or causing the disruption of a computer, computer system, or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system, or network.

(6) Preventing a computer user from exiting a site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system.

(7) Obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system, or network that is operated by this state, a political subdivision of this state, or a medical institution.

(8) Giving a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the consent of the person using the computer security system to restrict access to a computer, computer network, computer system, or data.

(b)(1) Except as otherwise provided in this subsection, the offense of computer tampering is a Class A misdemeanor, punishable as provided by law. Subsection (a) does not apply to any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his of her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) If the actor's intent is to commit an unlawful act or obtain a benefit, or defraud or harm another, the offense is a Class C felony, punishable as provided by law.

(3) If any violation results in a victim expenditure of greater than two thousand five hundred dollars ($2,500), or if the actor's intent is to obtain a benefit, commit an unlawful act, or defraud or harm another and there is an interruption or impairment of governmental operations or public communication, transportation, or supply of water, gas, or other public or utility service, the offense is a Class B felony, punishable as provided by law.

(4) If any violation results in a victim expenditure of greater than one hundred thousand dollars ($100,000), or if the committed offense causes physical injury to any person who is not involved in the act, the offense is a Class A felony, punishable as provided by law.

(5) If any violation relates to access to an Alabama Criminal Justice Information Center information system or to data regulated under the authority of the Alabama Justice Information Commission, the offense is a Class B felony, punishable as provided by law. Misuse of each individual record constitutes a separate offense under this subsection.

(c) A prosecution for a violation of this section may be tried in any of the following:

(1) The county in which the victimized computer, computer system, or network is located.

(2) The county in which the computer, computer system, or network that was used in the commission of the offense is located or in which any books, records, documents, property, financial instruments, computer software, data, access devices, or instruments of the offense were used.

(3) The county in which any authorized user was denied service or in which an authorized user's service was interrupted.

(4) The county in which critical infrastructure resources were tampered with or affected.

(Act 2012-432, p. 1192, §3.)

Section 13A-8-113

Encoded data fraud.

(a) A person commits the crime of encoded data fraud by:

(1) Knowingly and with the intent to commit an unlawful act or to defraud, possessing a scanning device; or knowingly and with intent to commit an unlawful act or defraud, using or attempting to use a scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on an identification document by means of magnetic strip, integrated circuit, or radio frequency identification tag without the permission of the authorized user or issuer of the identification document.

(2) Knowingly and with the intent to commit an unlawful act or to defraud, possessing a reencoder; or knowingly and with

intent to commit an unlawful act or defraud, using or attempting to use a reencoder to place encoded information on an identification document by means of magnetic strip, integrated circuit, or radio frequency identification tag without the permission of the authorized user or issuer of the identification document from which the information is being reencoded.

(3) Knowingly and with intent to commit an unlawful act or to defraud, possess any purported credit or debit card that was not legitimately issued by a financial institution, company, governmental agency, or other card issuer. If any credit or debit card contains conflicting identifying information, this conflict shall create a rebuttable presumption of intent to commit an unlawful act or to defraud and that the credit or debit card was not legitimately issued.

(b) Any person violating this section, upon conviction, shall be guilty of a Class C felony. For the purposes of charges under subdivision (3) of subsection (a), the possession of each credit or debit card shall be charged as a separate count.

(c) Any scanning device, reencoder, or credit or debit card owned by the defendant and possessed or used in violation of this section may be seized and be destroyed as contraband by the investigating law enforcement agency by which the scanning device, reencoder, or credit or debit card was seized.

(Act 2012-432, p. 1192, §4; Act 2016-359, §1.)

Section 13A-8-114

Phishing.

(a) A person commits the crime of phishing if the person by means of an Internet web page, electronic mail message, or otherwise using the Internet, solicits, requests, or takes any action to induce another person to provide identifying information by representing that the person, either directly or by implication, is a business, without the authority or approval of the business.

(b) Any person violating this section, upon conviction, shall be guilty of a Class C felony. Multiple violations resulting from a single action or act shall constitute one violation for the purposes of this section.

(c) The following persons may bring an action against a person who violates or is in violation of this section:

(1) A person who is engaged in the business of providing Internet access service to the public, owns a web page, or owns a trademark, and is adversely affected by a violation of this section.

(2) An individual who is adversely affected by a violation of this section.

(d) In any criminal proceeding brought pursuant to this section, the crime shall be considered to be committed in any

county in which any part of the crime took place, regardless of whether the defendant was ever actually present in that county, or in the county of residence of the person who is the subject of the identification documents or identifying information.

(e) The Attorney General or the district attorney may file a civil action in circuit court to enforce this section and to enjoin further violations of this section. The Attorney General or the district attorney may recover actual damages or twenty-five thousand dollars ($25,000), whichever is greater, for each violation of subsection (a).

(f) In a civil action under subsection (e), the court may increase the damage award to an amount equal to not more than three times the award provided in subsection (d) if the court determines that the defendant has engaged in a pattern and practice of violating subsection (a).

(g) Proceeds from an action under subsection (e) shall first be used for payment of all proper expenses, including court costs, of the proceedings for the civil action with the remaining proceeds payable first towards the restitution of any victims, as determined by the court. Any remaining proceeds shall be awarded equally between the State General Fund and the office of the Attorney General, the office of the district attorney bringing the action, or both.

(h) An interactive computer service provider shall not be held liable or found in violation of this section for identifying, removing, or disabling access to an Internet web page or other online location that such provider reasonably believes by clear and convincing evidence that it is being used to engage in a violation of this section.

(Act 2012-432, p. 1192, §5.)

Section 13A-8-115

Disclosure of stored wire or electronic communications, transaction records, etc.

(a) A law enforcement officer, a prosecuting attorney, or the Attorney General may require the disclosure of stored wire or electronic communications, as well as transactional records and subscriber information pertaining thereto, to the extent and under the procedures and conditions provided for by the laws of the United States.

(b) A provider of electronic communication service or remote computing service shall provide subscriber information as well as the contents of, and transactional records pertaining to, wire and electronic communications in its possession or reasonably accessible thereto when a requesting law enforcement officer, a prosecuting attorney, or the Attorney General complies with the provisions for access thereto set forth by the laws of the United States.

(c) Warrants or appropriate orders for production of stored wire or electronic communications and transactional records pertaining thereto shall have statewide application or application as provided by the laws of the United States when issued

by a judge with jurisdiction over the criminal offense under investigation or to which such records relate.

(d) This section specifically authorizes any law enforcement official, prosecuting attorney, or the Attorney General to issue a subpoena to obtain any stored electronic records governed by 18 U.S.C. § 2703(b) et seq., and any successor statute. The subpoena shall be issued with a showing that the subpoenaed material relates to an investigation.

(e) Intentional violation of this section shall be punishable as contempt.

(Act 2012-432, p. 1192, §6.)

Section 13A-8-116

Warrants from other states.

(a) An Alabama corporation or business entity that provides electronic communication services or remote computing services to the general public, when served with a warrant issued by another state to produce records that could reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant had been issued by an Alabama court.

(b) Intentional violation of this section shall be punishable as contempt.

(Act 2012-432, p. 1192, §7.)

Section 13A-8-117

Forfeiture of certain computers, software, etc.

(a) On conviction of a violation of this article or any other violation of the criminal laws of Alabama, the court shall order that any computer, computer system, computer network, instrument of communication, software or data that was owned or used by the defendant with the owner's knowledge of the unlawful act or where the owner had reason to know of the unlawful act, and that was used in the commission of the offense be forfeited to the State of Alabama and sold, destroyed, or otherwise properly disposed. If the defendant is a minor, it also includes the above listed property of the parent or guardian of the defendant. The manner, method, and procedure for the forfeiture and condemnation or forfeiture of such thing shall be the same as that provided by law for the confiscation or condemnation or forfeiture of automobiles, conveyances, or vehicles in which alcoholic beverages are illegally transported. If the computer, computer system, computer network, instrument of communication, software, or data that was used by a defendant, in conjunction with a violation of this article, is owned or leased by the defendant's employer or a client or vendor of the defendant's employer and such owner or lessor did not authorize the activity violating the article, this section shall not apply.

(b) When property is forfeited under this article or any other violation of the criminal laws of Alabama, the court may

award the property to any state, county, or municipal law enforcement agency or department who participated in the investigation or prosecution of the offense given rise to the seizure. The recipient law enforcement agency shall use such property for law enforcement purposes but, at its discretion, may transfer the tangible property to another governmental department or agency to support crime prevention. The agencies may sell that which is not required to be destroyed and which is not harmful to the public. The proceeds from a sale authorized by this article shall be used first for payment of all proper expenses of the proceedings for forfeiture and sale and the remaining proceeds from the sale shall be awarded and distributed by the court to the participating agencies to be used exclusively for law enforcement purposes.

(c) Pursuant to Section 15-18-67, and in addition to any other cost ordered pursuant to law, the district attorney may request and the court may order the defendant to pay the cost of prosecution or investigation, or both. Restitution shall include any and all costs associated with the violation of the criminal laws of this state.

(Act 2012-432, p. 1192, §8.)

Section 13A-8-118

Prosecution.

A person who is subject to prosecution under this article and any other law of this state may be prosecuted under either or both laws.

(Act 2012-432, p. 1192, §9.)

Section 13A-8-119

Activities of law enforcement agencies, political subdivisions, etc.

Nothing in this article prohibits any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of this state or a political subdivision of this state or a law enforcement agency of the United States or of an intelligence agency of the United States.

(Act 2012-432, p. 1192, §10.)