Article 60.

Computer-Related Crime.

**§ 14-453. Definitions.**

As used in this Article, unless the context clearly requires otherwise, the following terms have the meanings specified:

(1) "Access" means to instruct, communicate with, cause input, cause output, cause data processing, or otherwise make use of any resources of a computer, computer system, or computer network.

(1a) "Authorization" means having the consent or permission of the owner, or of the person licensed or authorized by the owner to grant consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

(1b) "Commercial electronic mail" means messages sent and received electronically consisting of commercial advertising material, the principal purpose of which is to promote the for-profit sale or lease of goods or services to the recipient.

(2) "Computer" means an internally programmed, automatic device that performs data processing or telephone switching.

(3) "Computer network" means the interconnection of communication systems with a computer through remote terminals, or a complex consisting of two or more interconnected computers or telephone switching equipment.

(4) "Computer program" means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data.

(4a) "Computer services" means computer time or services, including data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection with any of these services.

(5) "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer, computer system, or computer network.

(6) "Computer system" means at least one computer together with a set of related, connected, or unconnected peripheral devices.

(6a) "Data" means a representation of information, facts, knowledge, concepts, or instructions prepared in a formalized or other manner and intended for use in a computer, computer system, or computer network. Data may be embodied in any form including computer printouts, magnetic storage media, optical storage media, and punch cards, or may be stored internally in the memory of a computer.

(6b) "Electronic mail" means the same as the term is defined in G.S. 14-196.3(a)(2).

(6c) "Electronic mail service provider" means any person who (i) is an intermediary in sending or receiving electronic mail and (ii) provides to end users of electronic mail services the ability to send or receive electronic mail.

(7) "Financial instrument" includes any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card or marketable security, or any electronic data processing representation thereof.

(7a) "Government computer" means any computer, computer program, computer system, computer network, or any part thereof, that is owned, operated, or used by any State or local governmental entity.

(7b) "Internet chat room" means a computer service allowing two or more users to communicate with each other in real time.

(7c) "Profile" means (i) a configuration of user data required by a computer so that the user may access programs or services and have the desired functionality on that computer or (ii) a Web site user's personal page or section of a page made up of data, in text or graphical form, which displays significant, unique, or identifying information, including, but not limited to, listing acquaintances, interests, associations, activities, or personal statements.

(8) "Property" includes financial instruments, information, including electronically processed or produced data, and computer software and computer programs in either machine or human readable form, and any other tangible or intangible item of value.

(8a) "Resource" includes peripheral devices, computer software, computer programs, and data, and means to be a part of a computer, computer system, or computer network.

(9) "Services" includes computer time, data processing and storage functions.

(10) "Unsolicited" means not addressed to a recipient with whom the initiator has an existing business or personal relationship and not sent at the request of, or with the express consent of, the recipient. (1979, c. 831, s. 1; 1993 (Reg. Sess., 1994), c. 764, s. 1; 1999-212, s. 2; 2000-125, s. 3; 2002-157, s. 1; 2009-551, s. 2; 2012-149, s. 2.)

**§ 14-453.1. Exceptions.**

This Article does not apply to or prohibit:

(1) Any terms or conditions in a contract or license related to a computer, computer network, software, computer system, database, or telecommunication device; or

(2) Any software or hardware designed to allow a computer, computer network, software, computer system, database, information, or telecommunication service to operate in the ordinary course of a lawful business or that is designed to allow an owner or authorized holder of information to protect data, information, or rights in it. (2002-157, s. 2.)

**§ 14-453.2. Jurisdiction.**

Any offense under this Article committed by the use of electronic communication may be deemed to have been committed where the electronic communication was originally sent or where it was originally received in this State. "Electronic communication" means the same as the term is defined in G.S. 14-196.3(a). (2002-157, s. 3.)

**§ 14-454. Accessing computers.**

(a) It is unlawful to willfully, directly or indirectly, access or cause to be accessed any computer, computer program, computer system, computer network, or any part thereof, for the purpose of:

(1) Devising or executing any scheme or artifice to defraud, unless the object of the scheme or artifice is to obtain educational testing material, a false educational testing score, or a false academic or vocational grade, or

(2) Obtaining property or services other than educational testing material, a false educational testing score, or a false academic or vocational grade for a person, by means of false or fraudulent pretenses, representations or promises.

A violation of this subsection is a Class G felony if the fraudulent scheme or artifice results in damage of more than one thousand dollars ($1,000), or if the property or services obtained are worth more than one thousand dollars ($1,000). Any other violation of this subsection is a Class 1 misdemeanor.

(b) Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any computer, computer program, computer system, or computer network for any purpose other than those set forth in subsection (a) above, is guilty of a Class 1 misdemeanor.

(c) For the purpose of this section, the phrase "access or cause to be accessed" includes introducing, directly or indirectly, a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system, or computer network. (1979, c. 831, s. 1; 1979, 2nd Sess., c. 1316, s. 19; 1981, cc. 63, 179; 1993, c. 539, s. 293; 1994, Ex. Sess., c. 24, s. 14(c); 1993 (Reg. Sess., 1994), c. 764, s. 1; 2000-125, s. 4.)

**§ 14-454.1. Accessing government computers.**

(a) It is unlawful to willfully, directly or indirectly, access or cause to be accessed any government computer for the purpose of:

(1) Devising or executing any scheme or artifice to defraud, or

(2) Obtaining property or services by means of false or fraudulent pretenses, representations, or promises.

A violation of this subsection is a Class F felony.

(b) Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any government computer for any purpose other than those set forth in subsection (a) of this section is guilty of a Class H felony.

(c) Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any educational testing material or academic or vocational testing scores or grades that are in a government computer is guilty of a Class 1 misdemeanor.

(d) For the purpose of this section the phrase "access or cause to be accessed" includes introducing, directly or indirectly, a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system, or computer network. (2002-157, s. 4.)

**§ 14-455. Damaging computers, computer programs, computer systems, computer networks, and resources.**

(a) It is unlawful to willfully and without authorization alter, damage, or destroy a computer, computer program, computer system, computer network, or any part thereof. A violation of this subsection is a Class G felony if the damage caused by the alteration, damage, or destruction is more than one thousand dollars ($1,000). Any other violation of this subsection is a Class 1 misdemeanor.

(a1) It is unlawful to willfully and without authorization alter, damage, or destroy a government computer. A violation of this subsection is a Class F felony.

(b) This section applies to alteration, damage, or destruction effectuated by introducing, directly or indirectly, a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system, or computer network. (1979, c. 831, s. 1; 1979, 2nd Sess., c. 1316, s. 20; 1981, cc. 63, 179; 1993, c. 539, s. 294; 1994, Ex. Sess., c. 24, s. 14(c); 1993 (Reg. Sess., 1994), c. 764, s. 1; 1995, c. 509, s. 12; 2000-125, s. 5; 2002-157, s. 5.)

**§ 14-456. Denial of computer services to an authorized user.**

(a) Any person who willfully and without authorization denies or causes the denial of computer, computer program, computer system, or computer network services to an authorized user of the computer, computer program, computer system, or computer network services is guilty of a Class 1 misdemeanor.

(b) This section also applies to denial of services effectuated by introducing, directly or indirectly, a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system, or computer network. (1979, c. 831, s. 1; 1993, c. 539, s. 295; 1994, Ex. Sess., c. 24, s. 14(c); 1993 (Reg. Sess., 1994), c. 764, s. 1; 2000-125, s. 6.)

**§ 14-456.1. Denial of government computer services to an authorized user.**

(a) Any person who willfully and without authorization denies or causes the denial of government computer services is guilty of a Class H felony. For the purposes of this section, the term "government computer service" means any service provided or performed by a government computer as defined in G.S. 14-454.1.

(b) This section also applies to denial of services effectuated by introducing, directly or indirectly, a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system, or computer network. (2002-157, s. 6.)

**§ 14-457. Extortion.**

Any person who verbally or by a written or printed communication, maliciously threatens to commit an act described in G.S. 14-455 with the intent to extort money or any pecuniary advantage, or with the intent to compel any person to do or refrain from doing any act against his will, is guilty of a Class H felony. (1979, c. 831, s. 1; 1979, 2nd Sess., c. 1316, s. 21; 1981, cc. 63, 179.)

**§ 14-458. Computer trespass; penalty.**

(a) Except as otherwise made unlawful by this Article, it shall be unlawful for any person to use a computer or computer network without authority and with the intent to do any of the following:

(1) Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network.

(2) Cause a computer to malfunction, regardless of how long the malfunction persists.

(3) Alter or erase any computer data, computer programs, or computer software.
(4) Cause physical injury to the property of another.
(5) Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.
(6) Falsely identify with the intent to deceive or defraud the recipient or forge commercial electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk commercial electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

For purposes of this subsection, a person is "without authority" when (i) the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission, or (ii) the person uses a computer or computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk commercial electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider.

(b) Any person who violates this section shall be guilty of computer trespass, which offense shall be punishable as a Class 3 misdemeanor. If there is damage to the property of another and the damage is valued at less than two thousand five hundred dollars ($2,500) caused by the person's act in violation of this section, the offense shall be punished as a Class 1 misdemeanor. If there is damage to the property of another valued at two thousand five hundred dollars ($2,500) or more caused by the person's act in violation of this section, the offense shall be punished as a Class I felony.

(c) Any person whose property or person is injured by reason of a violation of this section may sue for and recover any damages sustained and the costs of the suit pursuant to G.S. 1-539.2A.

(d) It is not a violation of this section for a person to act pursuant to Chapter 36F of the General Statutes. (1999-212, s. 3; 2000-125, s. 7; 2016-53, s. 2.)

**§ 14-458.1. Cyber-bullying; penalty.**

(a) Except as otherwise made unlawful by this Article, it shall be unlawful for any person to use a computer or computer network to do any of the following:

(1) With the intent to intimidate or torment a minor:
  a. Build a fake profile or Web site;
  b. Pose as a minor in:
    1. An Internet chat room;
    2. An electronic mail message; or
    3. An instant message;
  c. Follow a minor online or into an Internet chat room; or
  d. Post or encourage others to post on the Internet private, personal, or sexual information pertaining to a minor.
(2) With the intent to intimidate or torment a minor or the minor's parent or guardian:
  a. Post a real or doctored image of a minor on the Internet;

b. Access, alter, or erase any computer network, computer data, computer program, or computer software, including breaking into a password protected account or stealing or otherwise accessing passwords; or

c. Use a computer system for repeated, continuing, or sustained electronic communications, including electronic mail or other transmissions, to a minor.

(3) Make any statement, whether true or false, intending to immediately provoke, and that is likely to provoke, any third party to stalk or harass a minor.

(4) Copy and disseminate, or cause to be made, an unauthorized copy of any data pertaining to a minor for the purpose of intimidating or tormenting that minor (in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network).

(5) Sign up a minor for a pornographic Internet site with the intent to intimidate or torment the minor.

(6) Without authorization of the minor or the minor's parent or guardian, sign up a minor for electronic mailing lists or to receive junk electronic messages and instant messages, with the intent to intimidate or torment the minor.

(b) Any person who violates this section shall be guilty of cyber-bullying, which offense shall be punishable as a Class 1 misdemeanor if the defendant is 18 years of age or older at the time the offense is committed. If the defendant is under the age of 18 at the time the offense is committed, the offense shall be punishable as a Class 2 misdemeanor.

(c) Whenever any person pleads guilty to or is guilty of an offense under this section, and the offense was committed before the person attained the age of 18 years, the court may, without entering a judgment of guilt and with the consent of the defendant, defer further proceedings and place the defendant on probation upon such reasonable terms and conditions as the court may require. Upon fulfillment of the terms and conditions of the probation provided for in this subsection, the court shall discharge the defendant and dismiss the proceedings against the defendant. Discharge and dismissal under this subsection shall be without court adjudication of guilt and shall not be deemed a conviction for purposes of this section or for purposes of disqualifications or disabilities imposed by law upon conviction of a crime. Upon discharge and dismissal pursuant to this subsection, the person may apply for an order to expunge the complete record of the proceedings resulting in the dismissal and discharge, pursuant to the procedures and requirements set forth in G.S. 15A-146. (2009-551, s. 1; 2012-149, s. 3.)

**§ 14-458.2. Cyber-bullying of school employee by student; penalty.**

(a) The following definitions apply in this section:

(1) School employee. – The term means any of the following:

a. An employee of a local board of education, a charter school authorized under G.S. 115C-218.5, a regional school created under G.S. 115C-238.62, a laboratory school created under G.S. 116-239.7, or a nonpublic school which has filed intent to operate under Part 1 or Part 2 of Article 39 of Chapter 115C of the General Statutes.

b. An independent contractor or an employee of an independent contractor of a local board of education, a charter school authorized under G.S. 115C-218.5, a regional school created under G.S. 115C-238.62, a

laboratory school created under G.S. 116-239.7, or a nonpublic school which has filed intent to operate under Part 1 or Part 2 of Article 39 of Chapter 115C of the General Statutes, if the independent contractor carries out duties customarily performed by employees of the school.

(2) Student. – A person who has been assigned to a school by a local board of education as provided in G.S. 115C-366 or has enrolled in a charter school authorized under G.S. 115C-218.5, a regional school created under G.S. 115C-238.62, a laboratory school created under G.S. 116-239.7, or a nonpublic school which has filed intent to operate under Part 1 or Part 2 of Article 39 of Chapter 115C of the General Statutes, or a person who has been suspended or expelled from any of those schools within the last year.

(b) Except as otherwise made unlawful by this Article, it shall be unlawful for any student to use a computer or computer network to do any of the following:

(1) With the intent to intimidate or torment a school employee, do any of the following:
   a. Build a fake profile or Web site.
   b. Post or encourage others to post on the Internet private, personal, or sexual information pertaining to a school employee.
   c. Post a real or doctored image of the school employee on the Internet.
   d. Access, alter, or erase any computer network, computer data, computer program, or computer software, including breaking into a password-protected account or stealing or otherwise accessing passwords.
   e. Use a computer system for repeated, continuing, or sustained electronic communications, including electronic mail or other transmissions, to a school employee.

(2) Make any statement, whether true or false, intending to immediately provoke, and that is likely to provoke, any third party to stalk or harass a school employee.

(3) Copy and disseminate, or cause to be made, an unauthorized copy of any data pertaining to a school employee for the purpose of intimidating or tormenting that school employee (in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network).

(4) Sign up a school employee for a pornographic Internet site with the intent to intimidate or torment the employee.

(5) Without authorization of the school employee, sign up a school employee for electronic mailing lists or to receive junk electronic messages and instant messages, with the intent to intimidate or torment the school employee.

(c) Any student who violates this section is guilty of cyber-bullying a school employee, which offense is punishable as a Class 2 misdemeanor.

(d) Whenever any student pleads guilty to or is guilty of an offense under this section, the court may, without entering a judgment of guilt and with the consent of the student, defer further proceedings and place the student on probation upon such reasonable terms and conditions as the court may require. Upon fulfillment of the terms and conditions of the probation provided for in

this subsection, the court shall discharge the student and dismiss the proceedings against the student. Discharge and dismissal under this subsection shall be without court adjudication of guilt and shall not be deemed a conviction for purposes of this section or for purposes of disqualifications or disabilities imposed by law upon conviction of a crime. Upon discharge and dismissal pursuant to this subsection, the student may apply for an order to expunge the complete record of the proceedings resulting in the dismissal and discharge, pursuant to the procedures and requirements set forth in G.S. 15A-146.

(e) Whenever a complaint is received pursuant to Article 17 of Chapter 7B of the General Statutes based upon a student's violation of this section, the juvenile may, upon a finding of legal sufficiency pursuant to G.S. 7B-1706, enter into a diversion contract pursuant to G.S. 7B-1706. (2012-149, s. 4; 2014-101, s. 7; 2016-94, s. 11.6(b); 2017-117, s. 2.)

**§ 14-459. Reserved for future codification purposes.**