Section 28.1 Purpose

The Illinois Department of Children and Family Services recognizes that advances in technology have had a significant impact on almost every group of people throughout the world, including the many people served by the Department. On a daily basis information is easily shared electronically through social networking sites on the Internet, among desktop computers/tablets/laptops, and over cell phones via mobile web browsing and texting. This Administrative Procedure is intended to provide guidance to the identified primary users within the context of existing DCFS Rules and Procedures. To be effective, all primary users must receive ongoing training and education to ensure the protection and privacy of those who interact with the Department.

Section 28.2 Primary Users

Primary users of this Administrative Procedure are foster parents, relative caregivers, case-carrying staff of the Department and purchase of service agencies (including relative care, traditional foster care, specialized foster care, independent/transitional living agencies, and residential/group home care providers), DCFS and POS administrators, trainers, other child welfare personnel, and children who are youth in the care of the State of Illinois.
Section 28.3  Definitions

“Caregiver” is a relative foster parent, licensed foster parent, specialized foster parent, or a residential/group home care provider.

“Caseworker” is the assigned DCFS or purchase of services caseworker and/or supervisor for a DCFS youth in care.

“Cyberbullying” is the use of interactive technology to harass, threaten, embarrass or target another person. When an adult is involved, such action may be classified as “cyber-harassment” or “cyber-stalking;” both actions are considered crimes, and have legal consequences, including possible incarceration. (See www.kidshealth.org and Appendix B generally.)

“COPPA” (The Children’s Online Privacy Protection Act 15 U.S.C. §§6501-6506) is an Act of Congress designed to ensure that parents and guardians have control over what information is collected from their children online.

“Identity Theft” is a form of stealing someone’s identity, e.g., name and social security number, in which someone pretends to be someone else by assuming that person’s identity. Usually this is done to commit fraud, theft and other crimes against the victim whose identity is illegally used.

“Legal custody” means the relationship created by court order, in the best interests of a minor, that imposes on the custodian the responsibility of physical custody of a minor and the duty to protect, train and discipline that minor, and to provide that minor with food, clothing, shelter, education and ordinary and routine medical care.

“Mobile Technology” refers to the use of social media/texting with a mobile device.

"Sexting" is the practice of sending nude or semi-nude images/pictures, or images/pictures that indicate sexual activities, by cell phone or other electronic media; it is a sexual text ('sext') message.

“Sex Trafficking” means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act.

“Social Media” means current and future interactive technologies including, but not limited to, text, audio, video, images, podcasts, and other multimedia communications, in virtual communities and online networks.

“Unique identifiers” means information including but not limited to a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses.
“Youth” or “Youth in care” is a child for whom the Department is legally responsible. This means a child for whom the Department has temporary protective custody, custody or guardianship via court order, or a child whose parents have signed an adoptive surrender or voluntary placement agreement with the Department.

Section 28.4 Background

Society is moving toward a greater reliance on digital communication. Unlike other forms of communication, almost any digital communication can become public and permanent. With a single key stroke, personal information may become immediately accessible by anyone.

At the same time, DCFS Rules and Procedures continue to protect the confidentiality of persons served by the Department. “No personal information obtained concerning a person served by the Department or concerning the subjects of a child abuse or neglect report may be disclosed by the Department without the written consent of that individual, provided that individual has reached 18 years of age…” (See DCFS Rule 431.40 a)

Likewise, criminal and civil statutes apply to digital communications. Minors and adults who use electronic communications to convey information that is indecent, intimidating or abusive may be arrested and criminally prosecuted. Criminal offenses such as bullying, stalking, child pornography and fraud remain criminal offenses when committed through use of digital technology. An on-line purchase, like an in-store purchase, is subject to interest and penalties if payment is delayed. (See Appendix B for a partial list of possible offenses.)

Illinois child welfare laws also establish the general responsibilities of a minor’s legal custodian or guardian and define the rights and responsibilities of foster parents to the youth entrusted in their care. These laws also apply to digital communication. While foster parents are not authorized to provide formal legal consents on behalf of the minors placed in their homes, they are legally required to maintain a safe foster home environment, to appropriately care for and adequately supervise the children in their care, to handle discipline without delay, and in accordance with DCFS Rule and Procedure, they should encourage appropriate forms of indoor and outdoor recreation. (See the Illinois Juvenile Court Act 705 ILCS 405/1-2, the Children and Family Services Act 505 ILCS 20, the Illinois Foster Parent Code 89 Il. Adm. Code Parts 340, DCFS Procedures 340, Licensing Standards for Foster Family Homes.89 Il. Adm. Code Part 402 and DCFS Procedures 402.)

Finally, the Children’s Online Privacy Protection Act [15 U.S.C. §§6501-6506] or COPPA, provides young children with some additional identity protection. COPPA makes it a federal crime for operators of commercial websites, online services and mobile apps to collect, use or disclose the personal information of any child under the age of thirteen. However, COPPA does not protect the personal information of users over the age of thirteen; providers of web-sites, online services and mobile apps are free to gather personal information of users over 13 years of age and share it with any person, company or entity.
Confidentiality, criminal laws, civil laws, and federal protections must be considered in all digital communications.

General Rule: If something applies in the real world, it also applies in the digital world.

Section 28.5 Applicability

A) Social Media Safety Agreement

DCFS has developed the CFS 2034, Social Media Safety Agreement, as a way to help establish rules concerning Social Media/Mobile Technology usage, discuss safety practices, and to help wards become more informed and safe users of Social Media/Mobile Technology. This agreement is for the caregiver and the youth. It is intended as a way to help establish rules concerning Social Media/Mobile Technology usage, discuss safety practices, and to help youth in care become more informed and safe users of Social Media/Mobile Technology.

The caseworker shall review the CFS 2034, Social Media Safety Agreement, with each caregiver and each youth age 10 and older. The caseworker shall ask the caregiver and youth to sign the Agreement if the youth in care will be using any Social Media/Mobile Technology. The caseworker may provide an extra copy of the Agreement (signed or unsigned) to the caregiver and youth as a record of their Agreement.

If the youth in care is known to be using the technology at an earlier age the CFS 2034, Social Media Safety Agreement, should be completed.

Upon placement to a new home/setting, a CFS 2034, Social Media Safety Agreement, will be established within the first 30 days. The caseworker will review the CFS 2034, Social Media Safety Agreement, with the youth and the caregiver at the caseworker’s first monthly visit. This agreement will be signed by the youth and the caregiver; both will be given a copy of the agreement, and a copy will be maintained in youth’s case file. At least annually and more often as needed, the caregiver, youth, and caseworker shall,

**ACTION:**

- **Caregiver** Review and sign the CFS 2034, Social Media Safety Agreement.
- **Youth** Review and sign the CFS 2034, Social Media Safety Agreement.
- **Caseworker** Review the CFS 2034, Social Media Safety Agreement, with the Caregiver and Youth.
B) Youth and Use of Social Media

DCFS youth in care may create online accounts (e.g., Facebook, Twitter, and so forth) provided that they meet the proper age requirements for each site. The DCFS Guardianship Administrator does not support a minor having a social networking account if the youth is below the age required to have an account. No person is authorized to give permission in place of the DCFS Guardianship Administrator.

Generally, if youth are allowed access to Social Media/Mobile Technology, the caregiver, youth, and caseworker shall,

ACTION:

Caregiver

Apply any existing parental controls that go with that technology.

Set parental controls for any computer that is used in the placement, when possible.

Make reasonable efforts to monitor the youth’s access and use of this technology for safety purposes. The caregiver could be the relative or licensed foster parent, the residential/group home staff, or ILO/TLP staff.

Set reasonable limits on the use of Social Media & Mobile Technology in the placement.

Meet with the youth and caseworker to read and sign the CFS 2034, Social Media Safety Agreement.

Youth

Meet with the caregiver and caseworker to read and sign the CFS 2034, Social Media Safety Agreement.

Abide by the house rules related to social media of the caregiver.

Caseworker

Meet with the caregiver and caseworker to review the CFS 2034, Social Media Safety Agreement.

Place the original, signed CFS 2034, Social Media Safety Agreement, in the case file.

Listen to the reasonable requests of the youth, but support the reasonable rules of the caregiver.
Use of Social Media or Mobile Technology at School

Local school districts may have their own rules and procedures regarding the use of the Internet, electronic devices, and cellular phones at their schools. Nothing in this Administrative Procedure is meant to overrule or limit a more restrictive local school district policy regarding social media or mobile technology. Youth in care are expected to follow the rules of their school regarding the use of social media or mobile technology while at school.

Youth in Care with Their Own Electronic Device(s)

If DCFS youth in care come into the caregiver’s home with his/her own electronic device (e.g., tablet, MP3 player, computer or cell phone) and it is discovered that this technology is being used inappropriately, the caregiver, youth, and caseworker shall,

ACTION:

<table>
<thead>
<tr>
<th>Role</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caregiver</td>
<td>Contact the caseworker about the incident(s). Review the CFS 2034, Social Media Safety Agreement, with the youth and the caseworker.</td>
</tr>
<tr>
<td>Youth</td>
<td>Review the CFS 2034, Social Media Safety Agreement, with the caregiver and the caseworker.</td>
</tr>
<tr>
<td>Caseworker</td>
<td>Review the CFS 2034, Social Media Safety Agreement, with the caregiver and the youth. If there is no CFS 2034 in the case file, schedule a time to meet with the caregiver and youth and create one. Speak to the DCFS youth about the appropriate use of the electronic device. If the device does not belong to the ward, attempt to locate the actual owner of the device to alert him or her of the inappropriate use of that equipment.</td>
</tr>
</tbody>
</table>
Youth In Care Using the Caregiver’s Electronic Device(s)

If a caregiver allows a DCFS youth in care to use the caregiver’s own electronic device(s) and the caregiver believes that this equipment is being misused, the caregiver, youth, and caseworker should,

**ACTION:**

**Caregiver**  
Revoking the use of that device. Schedule a meeting with the caseworker to report and discuss the misuse of the equipment.

Review the *CFS 2034, Social Media Safety Agreement*, with the youth and the caseworker.

**Youth**  
Review the *CFS 2034, Social Media Safety Agreement*, with the caregiver and the caseworker.

**Caseworker**  
Review the *CFS 2034, Social Media Safety Agreement*, with the caregiver and the youth. If there is no CFS 2034 in the case file, schedule a time to meet with the caregiver and youth and create one.

*Speak to the DCFS youth about the appropriate use of the applicable electronic device and the caregiver’s authority to impose consequences if there is any further misuse of that equipment.*

**C) Confidentiality**

Juvenile Court proceedings involving cases of abuse and neglect are completely confidential. It is illegal for anyone, other than Department employees and Contractual staff (under limited circumstances) to convey specific information about a case, identifying personal information about a DCFS youth, personal information regarding the clients, including the parents, or information regarding the foster parent(s) to a third party not entitled to that information. (See DCFS Rule & Procedure 431 Confidentiality of Persons Served by the Department, DCFS Administrative Procedure 20 Electronic Communication and Distribution, DCFS Rule 430 Foster Parent Rights and Responsibilities, Juvenile Court Act of 1987 705 ILCS 405/1-8.)

When confidential information is disseminated over any Social Media/Mobile Technology all control of that information is lost.
The following types of private information should never be released using social media/mobile technology. This list is not all inclusive:

- Unique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses. Private information includes home address and personal license plates, except as otherwise provided by law or when compiled without possibility of attribution to any person.

- The fact that someone is a youth in the care of the State of Illinois is protected confidential information. Dissemination of this type of information over Social Media/Mobile Technology is prohibited.

- Caregiver information including names, addresses, telephone numbers, and e-mail addresses is also confidential.

Caregivers and youth in the care should be able to benefit from the positive aspects of the Social Media/Mobile Technology while still maintaining the requirements of confidentiality.

For example, a caregiver can post on his/her Facebook account about a specific accomplishment of a youth in the caregiver’s home/placement as long as the caregiver does not specifically identify that child as a youth in the care of DCFS.

If there are suspected breaches of confidentiality, the caregiver, youth, and caseworker shall,

**ACTION:**

- **Caregiver** Notify the assigned caseworker/supervisor.
- **Youth** Notify the assigned caseworker/supervisor.
- **Caseworker** Contact the Regional DCFS Office of Legal Services.

**D) Images/Videos**

Access to cell phone cameras has made the creation of images and videos a simple task.

Caregivers, youth, and caseworkers should be mindful that the use of any photos of DCFS youth in any form, including any posted online images, should not identify those children as DCFS youth in care.
The DCFS Guardianship Administrator must consent, in advance, to the release of any image or picture of a DCFS youth if that youth is going to be identified as a youth in the care of DCFS in any publication, whether online or in print format.

Also, when a digital photo is posted, the location where the photo was taken may be embedded within the photo. Since identification of the location may constitute a violation of confidentiality, it is recommended that DCFS wards NOT post pictures of themselves online.

Once a photograph, image or video is on the Internet all control over it is lost.

Once a photograph, image or video is sent in a text message, all control over that photo, image, or video is lost.

**Cyberbullying, Sexting and Other Criminal Acts**

For photos, images and/or videos that may constitute cyberbullying, sexting or a criminal act, all Caregivers, Wards, and Caseworkers shall,

**ACTION:**

Follow the procedures outlined in Section G (Criminal Acts), Section H (Cyberbullying), Section I (Sexting), and section J (Child Exploitation/Human Trafficking) for any images or videos that may apply to those situations.

**E) Employee Email, Texting, Video Communications From Caseworkers**

**Email**

DCFS employees and Contractual staff who are authorized users of the Department’s electronic mail, Internet systems, and other data distribution methods, including private agencies using the DCFS network, Contractual employees and DCFS Staff may transmit personal information of persons served by the Department via Outlook E-mail only. All transmissions by authorized users must be made in accordance with Rules and Procedures 431, DCFS Administrative Procedure 20, the Social Work Code of Ethics and current law.

**Texting**

It is permissible to contact a DCFS youth or client via a text message, but no case specific details should be sent in that type of communication. For example, the caseworker could arrange a meeting, but not discuss the entire purpose for that meeting with client specific information.
Video Communications

It may be appropriate for child welfare professionals to use video communications technologies such as Skype, or its equivalent, to interact with their clients. These types of video communications are the equivalent of contacting someone via the telephone. This type of communication does not replace required in person contacts delineated in Procedures 315.110, but does offer additional visual contact with DCFS youth and clients.

Client information is not to be shared using any official Social Media/Mobile Technology for any non-work purpose.

Client information is not to be shared using any personal Social Media/Mobile Technology for any non-work purpose.

Contact with clients using official or personal Social Media/Mobile Technology for a non-work purpose is also prohibited.

If there are suspected inappropriate communications by the DCFS staff, Contractual staff, or by the caregiver, the caregiver, youth, and caseworker shall,

**ACTION:**

*Caregiver* Notify the assigned caseworker/supervisor.

*Youth* Notify the assigned caseworker/supervisor.

*Caseworker* Contact the Regional DCFS Office of Legal Services.

F) Court Orders

Court orders prohibiting certain types of contact must be followed. Postings, comments, emails, or texts that violate existing court orders are prohibited.

For example, a no contact order between two individuals also includes “no contact” over Social Media/Mobile Technology. Emails, texts, Facebook posts or direct messages, tweets, etc., could all be considered a violation of a no contact court order.

If a court order is violated or suspected of being violated, the caregiver, youth, and caseworker shall,

**ACTION:**

*Caregiver* Notify the assigned caseworker/supervisor.

*Youth* Notify the assigned caseworker/supervisor.

*Caseworker* Contact the Regional DCFS Office of Legal Services.
G) **Criminal Acts**

Postings, comments, emails, or texts using Social Media/Mobile Technology that contain information that is criminal in nature may result in criminal prosecution. (See Appendix B for partial list of criminal acts which include coercion/threats, intimidation, emotional abuse, stalking, exploitation, and bullying.)

If digital communications through Social Media/Mobile Technology are being used in suspected criminal activities the caregiver, youth, and caseworker shall,

**ACTION:**

- **Caregiver** Notify the assigned caseworker/supervisor.
- **Youth** Notify the caregiver and assigned caseworker/supervisor.
- **Caseworker** Contact the Regional DCFS Office of Legal Services

**NOTE:** *The caregiver, youth, or caseworker shall call 911 to contact the police when emergency situations develop requiring immediate action.*

Report any suspected child exploitation or Internet crimes against youth to the Attorney General’s High Tech Crimes Bureau immediately at:

**Office (312) 814-3762**  
**Fax (312) 814-8283**  
**100 W Randolph**  
**12th Floor**  
**Illinois Attorney General High Tech Crimes Bureau**  
**Chicago, IL. 60601**

H) **Cyberbullying**

“Cyberbullying” is the act of harassing, humiliating, or threatening another person using the Internet or a cell phone. Cyberbullying can have a serious impact on a person's life and behavior. The Internet can magnify the effects of hurtful comments, embarrassing photographs, and other common bullying tactics.

Warning signs of Cyberbullying:

a. A youth in care receives mean or threatening e-mail messages, text messages, or instant messages.

b. Someone has posted mean or hurtful things about a youth in care online.

c. Someone has forwarded a youth’s e-mails or text messages to another person without the youth’s permission.
d. Someone has altered a picture of a youth online.
e. Someone has taken pictures of a youth without the youth’s permission and posted the picture(s) online.
f. Someone has stolen a youth’s password and is sending messages, posting information or pretending to be the youth.
g. Someone has started an offensive blog about a youth.

If cyberbullying is suspected, the caregiver, youth, and caseworker shall,

**ACTION:**

**Youth**

Speak to your caregiver, your caseworker, or an adult immediately if you experience any of these warning signs.

**Caregiver**

Call 911 if the youth is in immediate danger.

Speak to the youth about the situation.

Preserve any electronic evidence.

Review the **CFS 2034, Social Media Safety Agreement**, with the youth and caseworker.

Report improper content and usage to the perpetrator’s Web site or Internet Service Provider. (Most Web sites and Internet service providers have a service agreement that prohibits members from using their service to harass or threaten others. Most Web sites and Internet Service Providers also supply a link to report this type of abuse.)

Inform the Caseworker of the possible bullying.

**Caseworker**

Speak to the youth about the situation.

Preserve any electronic evidence.

Review the **CFS 2034, Social Media Safety Agreement**, with the youth and caregiver.

Report improper content and usage to the perpetrator’s Web site or Internet Service Provider. (Most Web sites and Internet service providers have a service agreement that prohibits members from using their service to harass or threaten others. Most Web sites and Internet Service Providers also supply a link to report this type of abuse.)
Caregiver, Youth, or the Caseworker:

If you believe any person is being bullied online, call 1-888-414-7678 or email e-info@atg.state.il.us to contact an Internet Safety Specialist at the Illinois Attorney General’s Office.

I) Sexting

"Sexting" is the practice of sending nude or semi-nude pictures or pictures indicating sexual acts by cell phone or other electronic media; it is a sexual text ('sext') message. Under Illinois law, sexting is illegal and could result in Juvenile Court intervention. Sexting could also result in criminal prosecution for the crime of child pornography.

A minor (a person under 18) that sends, requests or receives indecent photos using a cell phone, a tablet, or a portable or mobile computer could be put under the supervision of the Juvenile Justice Division through Juvenile Court. The minor could be ordered to obtain counseling or other supportive services to address the situation and also be ordered to perform community service.

The Juvenile Court Act specifically states that:

Nothing in this Section shall be construed to prohibit a prosecution for disorderly conduct, public indecency, child pornography, a violation of Article 26.5 Harassing and Obscene Communications of the Criminal Code of 2012, or any other applicable provision of law.

If sexting has taken place or is suspected, the caregiver, youth, and caseworker shall,

ACTION:

Caregivers

Contact the caseworker.

Review the CFS 2034, Social Media Safety Agreement, with the youth and caseworker.

If you allow a DCFS youth to use your own electronic equipment and believe that this equipment is being misused, revoke the use of that equipment until you are able to report the misuse to the assigned worker or supervisor.

Youth

Review the CFS 2034, Social Media Safety Agreement, with the caregiver and the caseworker.

Caseworker

Review the CFS 2034, Social Media Safety Agreement, with the caregiver and the youth.

Contact the Regional DCFS Office of Legal Services.
J) Child Exploitation / Human Trafficking

While exploring the Internet, youth in care may be exposed to inappropriate material and conduct through the World Wide Web, e-mail, and chat rooms. Chat rooms pose a particularly serious threat. In chat rooms, remote users can carry on conversations anonymously, concealing their true identities. Taking advantage of this anonymity, child predators often make their first contact with victims through chat rooms and instant messages.

Additionally, the Internet has transformed the landscape of human trafficking. Traffickers use social media and other online tools to recruit victims, and in the case of sex trafficking, find and communicate with customers. Youth can be lured by sex traffickers who contact them on social media sites such as Facebook under the guise of becoming friends, or inviting him or her to a party. Traffickers can misrepresent their age or appearance so the youth will believe he or she is a peer, and thus engage in what seems to be a safe conversation. In an effort to prevent human trafficking, youth must be aware of what human trafficking is and how he or she might be engaged by a trafficker via social media. For more information about the prevention, identification, and response to human trafficking, refer to DCFS Procedures 302, Appendix C, and the human trafficking page on the DCFS D-Net under the Operations link.

According to the National Center for Missing and Exploited Children (NCMEC), 42% of youth (ages 10-17) reported being exposed to inappropriate content on the internet; 66% reported the exposure was unwanted; and 9% who received the unwanted exposure were “very or extremely upset.”

In an effort to prevent child exploitation, the caregiver, youth, and caseworker shall,

**ACTION:**

- **Caregiver** Review the CFS 2034, Social Media Safety Agreement, with the youth and caseworker.

- Set up agreements and guidelines about the safe use of Social Media/Mobile Technology.

- Understand the functions of the software programs the youth in your home/placement uses. If you do not understand these functions, ask the youth, or anyone else familiar with the programs, to teach you.

- Be aware of what Internet sites the youth in your home/placement is visiting. Investigate blocking or screening services provided by various Internet Service Providers (ISPs) and software programs.
Learn about everyone the youth in your home/placement meets online and discuss these relationships with the child.

Spend time online with the youth in your home/placement and discuss their online experiences just as you would ask them about their day.

Youth

Do not give out any personal information such as your address, telephone number, caregiver’s work address/telephone number, or the name or location of your school without your caregiver’s permission.

If you ever encounter something online that you do not understand or that makes you feel uncomfortable, tell your caregiver and/or caseworker immediately.

Never get together with someone you meet online without asking your caregiver’s permission first. If a meeting is planned, make sure it is in a public place and bring a caregiver along. Never meet an online “friend” alone.

Do not send any pictures of yourself to anyone without discussing this with your caregiver.

Do not respond to any message that makes you feel uncomfortable. It is not your fault if you get a message like that, and it is okay to tell your caregiver and/or caseworker no matter what it is.

Do not pick screen names that give away personal information.

Follow your caregiver’s rules for computer and online use. Always make sure it is okay before going online.

Remember that people may not be who they say they are online.

Caseworker

Speak to the youth and the caregiver about the situation.

Review the CFS 2034, Social Media Safety Agreement, with the youth and the caregiver.

Report online child exploitation, send an e-mail to: illinoisicactip@atg.state.il.us.

Report child pornography, send an e-mail to: reportchildporn@atg.state.il.us.
Report any suspected child exploitation or Internet crimes against youths to the Attorney General’s High Tech Crimes Bureau immediately.

The Illinois Attorney General’s Office is part of the Internet Crimes Against Children (ICAC) Taskforce.

CONTACT INFORMATION ILLINOIS ICAC

Illinois Crimes Against Children Taskforce
Office (312) 814-3762
Fax (312) 814-8283
100 W Randolph
12th Floor
Illinois Attorney General High Tech Crimes Bureau
Chicago, IL. 60601

Also contact the CyberTipline at www.cybertipline.com or call 1-800-843-5678 to report crimes against children, including online enticement of children for sexual acts, obscene material sent to a child, and child pornography.

K) Expenses from Use or Misuse of Social Media/Mobile Technology

Neither the Department nor the DCFS Guardianship Administrator is financially or legally responsible for any costs associated with wireless communications that violate existing laws or occur as a result of any act, error, submission or omission by minor’s foster parent or care provider (See DCFS Administrative Procedure 13.)

If the caregiver might be financially liable for costs associated with social media or mobile technology, the caregiver, youth, and caseworker shall,

ACTION:

Caregiver  Contact the caseworker/supervisor to find out about the requirements of the Foster Child Damage Reimbursement Program (DCFS Administrative Procedure 13.)

Review the CFS 2034, Social Media Safety Agreement, with the youth and caseworker.

Youth  Review the CFS 2034, Social Media Safety Agreement, with the caregiver and the caseworker.

Caseworker  Review the CFS 2034, Social Media Safety Agreement, with the caregiver and the youth.
Identity Theft

Identity theft occurs when someone uses personal information such as your name, Social Security number, or bank account number without your knowledge to commit fraud or theft.

If the caregiver or the youth believes that they may be the victim of identity theft or if they believe that their personal or financial information may have been compromised, the caregiver, youth, and caseworker shall,

ACTION:

Caregiver  Contact the caseworker/supervisor.

Call the toll-free Illinois Attorney General Identity Theft Hotline at: 1-866-999-5630 or 1-877-844-5461 (TTY).

Youth  Talk to your caregiver and caseworker.

Caseworker  Meet with the caregiver and caseworker to review the circumstances of the possible identity theft.

Call the toll-free Illinois Attorney General Identity Theft Hotline at: 1-866-999-5630 or 1-877-844-5461 (TTY).

L) “COPPA” The Children’s Online Privacy Protection Act

“COPPA” (The Children’s Online Privacy Protection Act 15 U.S.C. §§6501-6506) is an Act of Congress designed to ensure that parents and guardians have control over what information is collected from their children online.

If it is suspected that an Internet site is collecting information about a child under 13 without permission, the caregiver, youth, and caseworker shall,

ACTION:

Caregiver  Contact the caseworker/supervisor.

Youth  Talk to your caregiver.

Caseworker  Contact the Regional DCFS Office of Legal Services. The Regional Counsel from the DCFS Office of Legal Services will contact the DCFS Guardianship Administrator about taking action to protect a youth’s information.
This page intentionally left blank.
APPENDIX A – RESOURCES

DCFS will have its own Social Media/Mobile Technology training materials available online via webinars for child welfare staff, caregivers, and DCFS youth. (Additional reference material will be added to this section once DCFS gets its own training designed.)

DCFS will also have periodic in-service training available at various locations throughout the state.

- **www.onguardonline.gov** A federal government website dedicated to teaching online safety, security, and responsibility.
- **www.netsmartz.org** : NetSmartz Workshop is an interactive, educational program of the National Center for Missing & Exploited Children® (NCMEC) that provides age-appropriate resources to help teach children how to be safer on- and offline.
- **http://www.missingkids.com** : The National Center For Missing and Exploited Children
- **www.wiredsafety.org** : WiredSafety is an online safety, education, and help group.
- **www.aplatformforgood.org** A Platform for Good (PFG) is a project of the Family Online Safety Institute (FOSI) designed to help parents, teachers, and teens to connect, share, and do good online.

**Who to Contact if Your Child is in Danger**

- Local Police: If your child is in immediate danger, you should call **911**. Otherwise, you can call your local police's non-emergency number to report a problem.
- **www.cybertipline.com** or call **1-800-843-5678** to report crimes against children, including online enticement of children for sexual acts, obscene material sent to a child, and child pornography.

**Cyberbullying**

- **http://www.brainpop.com/technology/computersandinternet/cyberbullying**
- **www.stopcyberbullying.org**
- **www.cyberbully411.org**
- **www.commonsensemedia.org/cyberbullying**
- **http://kidshealth.org/parent/positive/talk/cyberbullying.html**
Websites for Kids and Teens

- www.onguardonline.gov: A federal government website dedicated to teaching online safety, security, and responsibility.
- www.nsteens.org: This is a NetSmartz site that teaches tweens and teens about making safer choices online.

Search Engines For Children

- www.kidsclick.org
- www.kidrex.org
- www.kidtopia.info

Illinois Attorney General


Attorney General Lisa Madigan created the first-ever Illinois Identity Theft Hotline. The hotline provides Illinoisans who have been victimized by identity theft with one-on-one assistance as they work to report the crime to local law enforcement and financial institutions, repair their credit, and prevent future problems.

If you have been the victim of identity theft or believe your personal or financial information may have been compromised, please call the toll-free Identity Theft Hotline at: **1-866-999-5630** or **1-877-844-5461 (TTY)**.

Identity Theft

Identity theft occurs when someone uses personal information such as your name, Social Security number, or bank account number without your knowledge to commit fraud or theft.

There is much more information available regarding identity theft, credit reporting and credit disputation at the web site of the **Office of the Illinois Attorney General**, including the following:

- Reporting Identity Theft as a Victim
- Protecting Your Privacy Online
- Fair Debt Collection
Cyber Bullying

Illinois Attorney General’s E-Info Hotline at 1-888-414-7678 or E-info@atg.state.il.us
www.ebully411.com


To report online child exploitation, send an e-mail to: illinoisicactip@atg.state.il.us.

To report child pornography, send an e-mail to: reportchildporn@atg.state.il.us.

To make an anonymous report click http://www.missingkids.com/cybertipline/ or call the CYBER TIPLINE at 1-800-843-5678.

CONTACT INFORMATION

Illinois Crimes Against Children Taskforce (ICAC)
Deputy Chief Michael Sullivan
High Tech Crimes Bureau
100 W Randolph, 12th Floor
Chicago, IL. 60601
(312) 814-3762 Office   (312) 814-8283 Fax

To report Online Scams

Office of the Illinois Attorney General
www.ag.state.il.us

Chicago
(800) 386-5438, TTY: (800) 964-3013

Springfield
(800) 243-0618, TTY: (877) 844-5461

Carbondale
(800) 243-0607, TTY: (877) 675-9339
APPENDIX B – CRIMINAL & CIVIL LAWS

The following table does not attempt to identify every illegal or improper use of electronic communications, but provides the name, citation, summary and consequences of Illinois criminal and civil laws that may impact persons served by the Department. Additional state laws, as well as federal statutes and local ordinances also regulate use of electronic communications and may impose penalties including fine or imprisonment. Although the information contained in the table is current as of the time of publication, all laws are subject to revision and change. Neither the table, nor its contents purport to provide legal advice of any kind.

CRIMINAL STATE LAWS

<table>
<thead>
<tr>
<th>NAME</th>
<th>Harassment through Electronic Communications</th>
</tr>
</thead>
</table>

**SUMMARY**

Harassment through electronic communications includes when a person uses electronic communication to: 1) make any obscene comment, request, suggestion, or proposal with the intention to offend; 2) interrupt the telephone service or electronic communication service of any person with intention to harass; 3) transmit to any person any file, document, or other communication which prevents that person from using telephone service or electronic communication device with intention to harass (even if this communication is not read in its entirety or at all); 4) transmit an electronic communication or knowingly encourage someone to transmit an electronic communication to harass another person who is under 13 years of age (regardless of whether that person consents to harassment; defendant has to be at least 16 years of age at the time of commissioning this offense); 5) use electronic communication to threaten injury to the person or the property of the person or to any of his or her family or household members; or 6) knowingly allowing any electronic communication device that you own to be used for any of the purposes aforementioned.

Article 26.5-4 adds that if there is any evidence that a person made additional telephone calls or engaged in additional electronic communications after having been requested by a named person or family or household member of that person to stop may be considered as evidence of an intent to harass unless disproved by evidence to the contrary.

**CONSEQUENCE**

A person who violates this law is guilty of Class B misdemeanor. A second violation count can lead to a Class A misdemeanor (minimum 14 days in jail or 240 hours of public or community service). A person violating this law can be guilty of a Class 4 felony if: 1) person has 3 or more prior violations in last 10 yrs of harassment through phone, electronic communications, or any similar offense; 2) if person has violated this law against the same victim or member of the victim’s family or household in other states; 3) at the time of the offense, the offender was under conditions of bail, probation, conditional discharge, mandatory supervised released, or was the subject of an order of protection in this or any other state prohibiting contact with the victim or any member of their family or household; 4) in the course of offense, offender threatened to kill the victim or any member of the victim’s family or household; 5) the person has been convicted in last 10 years of forcible felony; 6) the person was at least 18 years old at the time of the offense and victim was under 18 years old at that time; 7) the person may order any person convicted under this Article to submit to a psychiatric examination.
<table>
<thead>
<tr>
<th>NAME</th>
<th>Stalking</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>Stalking includes when a person knowingly engages in a “COURSE OF CONDUCT” directed at a specific person, and he or she knows or should know that this course of conduct would cause a reasonable person to: 1) fear for his or her safety or the safety of a third person; or 2) suffer other emotional distress. COURSE OF CONDUCT means 2 or more acts including but not limited to a person directly, indirectly or through other persons, by any action, method, device, or means follows, monitors, observes, surveils, threatens, or communicates to or about, a person engages in other non-consensual contact, or interferes with or damages a person’s property or pet. A course of conduct may include contact via electronic communications. Electronic communication means any transfer of signs, signals, writings, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system. Electronic communication includes transmissions by a computer through the Internet to another computer.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>Stalking is a Class 4 felony; a second or subsequent conviction is a Class 3 felony.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>Cyber Stalking</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>Engaging in a course of conduct using electronic communication directed at a specific person, and he or she knows or should know that would cause a reasonable person to: 1) fear for his or her safety or the safety of a third person: or 2) suffer other emotional distress. Knowingly and without lawful justification, on at least 2 occasions, harasses another person through use of electronic communication: 1) at any time transmits a threat or places that person or family member in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint and the threat is directed towards that person or a family member of that person; 2) knowingly solicits the commission of an act by any person that would violate this law. Knowingly and without lawful justification creates and maintains an Internet website which is accessible to one or more third parties for a period of at least 24 hours, and which contains statements harassing another person.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>First offense is Class 4 felony; second and subsequent conviction is Class 3 felony.</td>
</tr>
<tr>
<td>NAME</td>
<td>Minors Involved in Electronic Dissemination of Indecent Visual Depictions In Need of Supervision</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>A minor shall not distribute or circulate an indecent visual depiction of another minor through the use of a computer or electronic communication device. Electronic Communication Device means an electronic device, including but not limited to a wireless telephone, personal digital assistant, or a portable or mobile computer (e.g. tablet, kindle), that is capable of transmitting images or pictures. Indecent visual depiction means a depiction or portrayal in any pose, posture, or setting involving a lewd showing of the unclothed or see through clothed genitals, pubic area, buttocks, or if such person is female, a fully or partially developed breast of the person.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>A minor who violates this law may be subject to petition for adjudication and adjudged a minor in need of supervision. A minor found to be in need of supervision for this may be ordered to obtain counseling or other supportive services or be ordered to perform community service. There may be the possibility of being prosecuted for disorderly conduct, public indecency, or child pornography in the Criminal Code or any other applicable provision of law.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>Hate Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>A person commits a hate crime when, by reason of the actual or perceived race, color, creed, religion, ancestry, gender, sexual orientation, physical or mental disability, or national origin of another individual group of individuals, regardless of the existence of any other motivating factor or factors, he commits ASSAULT, BATTERY, AGGRAVATED ASSAULT, MISDEMEANOR THEFT, CRIMINAL TRESPASS TO RESIDENCE, REAL PROPERTY, OR VEHICLE, MISDEMEANOR CRIMINAL DAMAGE TO PROPERTY, MOB ACTION, DISORDERLY CONDUCT, HARRASSMENT BY PHONE, OR HARASSMENT THROUGH ELECTRONIC COMMUNICATIONS.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>First offense- Class 4 felony; Second or subsequent offenses- Class 2 felony Class 3 Felony for first offense if committed: in church, mosque or other building used for religious purposes; in a cemetery or placed used to memorialize the dead; in a school or educational facility; in a public park, or in any public way within 1,000 feet of these places. In addition to any sentence, the court shall order either restitution paid to victim or impose a fine up to $1,000. Victim may also bring civil action for damages, injunction or appropriate relief against the offender. Parents or legal guardians or other appointed guardians of an un-emancipated minor shall be liable for the amount of any judgment for actual damages rendered against such a minor.</td>
</tr>
<tr>
<td>NAME</td>
<td>False Personation; Solicitation</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>A person commits this offense if he or she knowingly and falsely represents himself or herself to be a member or representative of any veterans’ or public safety personnel organization or a representative of any charitable organization; or when they knowingly show or use in any manner any decal, badge, or insignia of any charitable, public safety personnel, or veterans’ organization without authorization. A person also commits false personation when they knowingly and falsely represent themselves to be: 1) another actual person and does an act in such assumed character with intent to intimidate, threaten, injure, defraud, or to obtain a benefit from another; or 2) a representative of an actual person or organization and does an act in such false capacity with intent to obtain a benefit or to injure or defraud another. This violation may be accomplished in person or by any means of communication, including but not limited to the use of an Internet website or any form of electronic communication.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>Violations can include being subjected to a fine of not less than $5 nor more than $100, or fines of at least $100 and not more than $200, or a Class C misdemeanor, or a Class A misdemeanor, or Class1-4 felony.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>Internet Offenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>ONLINE SALE OF STOLEN PROPERTY: a person commits online sale of stolen property when she accesses the internet with intent of selling property gained through unlawful means. ONLINE THEFT BY DECEPTION: using the Internet to purchase or attempt to purchase property from a seller with a mode of payment that he or she knows is fictitious, stolen, or lacking the consent of valid account holder. ELECTRONIC FENCING: selling stolen property using the Internet, knowing that the property was stolen. A person who unknowingly purchases stolen property over the Internet does not violate this law.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>Class 4 felony if full retail value of the stolen property or property obtained by deception does not exceed $300. Class 2 felony if full retail value exceeds $300.</td>
</tr>
<tr>
<td>NAME</td>
<td>Unauthorized video recording and live video transmission</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **SUMMARY**                      | It is unlawful for any person to knowingly make a video record or transmit live video of another person without that person’s consent:  
- in a restroom, tanning bed, tanning salon, locker room, changing room, or hotel bedroom.  
- in that other person’s residence.  
- in that other person’s residence when the recording or transmission is made outside that person’s residence by use of an audio or video device that records or transmits from a remote location.  
- under or through the clothing worn by that person for the purpose of viewing the body or the undergarments worn by that person.  
It is unlawful for any person to place or caused to be placed a device that makes a video record or transmits a live video:  
- in a locker room, changing room, or hotel bedroom with the intent to make a record or transmit live video of another person without that person’s consent.  
- with the intent to make a video record or transmit live video of another person in that other person’s residence without that person’s consent.  
It is unlawful for any person to, by any means, knowingly disseminate, or permit to be disseminated, a video record or live video that he or she knows to have been made or transmitted in violation of this offense.  
“Video Record” means and includes any videotape, photograph, film, or other electronic or digital recording of a still or moving visual image; and live video means and includes any real time or digital transmission of a still or moving visual image. |
| **CONSEQUENCE**                  | Sentencing for these violations range from Class A misdemeanor, Class 3 felony, Class 3 felony if the victim is under 18 or if the violation is committed by individual who is required to register as a sex offender. |

<table>
<thead>
<tr>
<th>NAME</th>
<th>Transmission of obscene messages</th>
</tr>
</thead>
</table>
| **SUMMARY**                      | A person commits transmission of obscene messages when he or she sends messages or uses language or terms which are **obscene, lewd or immoral with the intent to offend** through or when using a telephone, telegraph facilities, equipment or wires of any person, firm or corporation engaged in the transmission of news or messages between states or within the State of Illinois.  
The trier of fact may infer intent to offend from the use of language or terms which are obscene, lewd or immoral. |
| **CONSEQUENCE**                  | Not listed in statute |

---

Illinois Department of Children and Family Services  
Administrative Procedures #28 – (27)
<table>
<thead>
<tr>
<th>NAME</th>
<th>Harmful Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>A person is guilty of distributing harmful material to a minor when he or she:</td>
</tr>
<tr>
<td></td>
<td>• Knowingly sells, lends, distributes, exhibits to, depicts to, or gives away</td>
</tr>
<tr>
<td></td>
<td>to a minor, knowing that the minor is under the age of 18 or failing to</td>
</tr>
<tr>
<td></td>
<td>exercise reasonable care in ascertaining the person’s age:</td>
</tr>
<tr>
<td></td>
<td>• Any material which depicts nudity, sexual conduct, or sado-masochistic</td>
</tr>
<tr>
<td></td>
<td>abuse, or which contains explicit or detailed verbal descriptions or narrative</td>
</tr>
<tr>
<td></td>
<td>accounts of sexual excitement, sexual conduct or sado-masochistic abuse, and</td>
</tr>
<tr>
<td></td>
<td>which taken as a whole is harmful to minors:</td>
</tr>
<tr>
<td></td>
<td>• A motion picture, show, or other presentation which depicts nudity, sexual</td>
</tr>
<tr>
<td></td>
<td>conduct or sado-masochistic abuse and is harmful to minors:</td>
</tr>
<tr>
<td></td>
<td>• An admission ticket or pass to premises where there is exhibited or to be</td>
</tr>
<tr>
<td></td>
<td>exhibited such a motion picture, show, or other presentation; or</td>
</tr>
<tr>
<td></td>
<td>• Admits a minor to premises where there is exhibited or to be exhibited</td>
</tr>
<tr>
<td></td>
<td>such a motion picture, show, or other presentation, knowing that the minor is</td>
</tr>
<tr>
<td></td>
<td>a person under the age of 18 or failing to exercise reasonable care in ascertaining</td>
</tr>
<tr>
<td></td>
<td>the person’s true age.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>Distribution of harmful material in violation of this Section is a Class A</td>
</tr>
<tr>
<td></td>
<td>misdemeanor. A second or subsequent offense is a Class 4 felony. Any person</td>
</tr>
<tr>
<td></td>
<td>under the age of 18 who falsely states, either orally or in writing, that</td>
</tr>
<tr>
<td></td>
<td>he or she is not under the age of 18 (is an adult), or who presents or offers to</td>
</tr>
<tr>
<td></td>
<td>any person any false identification evidence or not actually his or her own in</td>
</tr>
<tr>
<td></td>
<td>order to order, obtain, view, or otherwise procure or attempt to view any harmful</td>
</tr>
<tr>
<td></td>
<td>material is guilty of a Class B misdemeanor. A person over the age of 18 who</td>
</tr>
<tr>
<td></td>
<td>fails to exercise reasonable care in ascertaining the true age of a minor,</td>
</tr>
<tr>
<td></td>
<td>knowingly distributes, or sends, or causes to be sent, or exhibits to, or offers</td>
</tr>
<tr>
<td></td>
<td>to distribute, or exhibits any harmful material to a person that he or she believes</td>
</tr>
<tr>
<td></td>
<td>is a minor is guilty of a Class A misdemeanor. If that person used a computer</td>
</tr>
<tr>
<td></td>
<td>web camera, cell phone, or any other type of device to make the harmful material,</td>
</tr>
<tr>
<td></td>
<td>then each offense is a Class 4 felony.</td>
</tr>
</tbody>
</table>
# ADMINISTRATIVE PROCEDURE #28
SOCIAL MEDIA/MOBILE TECHNOLOGY FOR CHILDREN/YOUTH IN CARE
April 17, 2014 – P.T. 2014.08

## CIVIL STATE LAWS

<table>
<thead>
<tr>
<th>NAME</th>
<th>Suspension or Expulsion of Pupils; School Searches</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>Impacts any student that has been determined to have made an explicit threat on an INTERNET website against a school employee, a student, or any school-related personnel; Impacts any student if the internet website through which the threat was made is a site accessible within the school at the time the threat was made or available to third parties who worked or studied within school grounds at the time the threat was made; and the threat could be reasonably interpreted as threatening to the safety and security of the threatened individual because his or her duties or employment status or status as a student inside the school.</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>The student may be suspended for a period not to exceed 10 school days or may be expelled for a definite period of time not to exceed 2 calendar years, as determined on a case by case basis.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>Electronic Paging Devices on School Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>No student shall use or have in his or her possession any pocket pager or similar electronic paging device while in any school building or on any school property, during regular school hours or at any other time, unless the use or possession of such device by such student has first been expressly authorized by the principal acting in accordance with standards developed as provided in subsection (c) for the granting of approved exceptions to the general prohibition of this Section against such use or possession. (c) The Board of Education shall develop and circulate written standards to each principal, under which a principal: (1) may authorize the use or possession of a pocket pager or similar electronic paging device by a student while in a school building or on school property as an approved exception to the general prohibition of this Section against such use or possession; and</td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>Principal may impose appropriate discipline or other sanctions against any student who violates this provision.</td>
</tr>
<tr>
<td>NAME</td>
<td>Transportation Vehicle Communication Devices</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>CITATION</td>
<td>Public Act 98-506 H.B. 1247; S.H.A 625 ILCS 5/12- 610.2</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>A person may not operate a motor vehicle on a roadway while using an electronic communication device. Electronic communication device means an electronic device, including but not limited to a hand held wireless telephone, hand held personal digital assistant, or a portable or mobile computer, BUT DOES NOT include a global positioning system (GPS) or navigation system or a devise that is physically or electronically integrated into the motor vehicle (e.g. Blue Tooth). This law does not apply to:</td>
</tr>
<tr>
<td>• Driver using electronic communication device for the sole purpose of reporting an emergency situation and continued communication with emergency personnel during the emergency situation;</td>
<td></td>
</tr>
<tr>
<td>• A driver using an electronic communication device in hands-free or voice operated mode, which may include the use of a headset;</td>
<td></td>
</tr>
<tr>
<td>• A driver using an electronic communication device whole parked on the shoulder of a roadway;</td>
<td></td>
</tr>
<tr>
<td>• A driver using an electronic communication device by pressing a single button to initiate or terminate a voice communication; or</td>
<td></td>
</tr>
<tr>
<td>• A driver using an electronic communication device capable of performing multiple functions, other than a hand held wireless telephone or hand held personal digital assistant (e.g. fleet management system, dispatching device, citizens band radio, or music player) for a purpose that is not otherwise prohibited by this law.</td>
<td></td>
</tr>
<tr>
<td>CONSEQUENCE</td>
<td>A second or subsequent violation is an offense against traffic regulations governing the movement of vehicles. A person who violates this law shall be fined a maximum of $75 for a first offense, $100 for a second offense, $125 for a third offense, and $150 for a fourth or subsequent offense.</td>
</tr>
</tbody>
</table>
**NAME** | Anti-Phishing Act  
--- | ---  
**SUMMARY** | It is unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing himself, herself, or itself to be a business without the authority or approval of the business.  
**CONSEQUENCE** | (a) The following persons may bring an action against a person who violates this act:  
(1) A person who (A) is engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark, and (B) is adversely affected by a violation of Section 10.  
An action brought under this paragraph may seek to recover the greater of actual damages or $500,000.  
(2) An individual who is adversely affected by a violation of Section 10 may bring an action, but only against a person who has directly violated Section 10.  
An action brought under this paragraph may seek to enjoin further violations of Section 10 and to recover the greater of 3 times the amount of actual damages or $5,000 per violation.  
(b) The Attorney General or a State's Attorney may bring an action against a person who violates or is in violation of Section 10 to enjoin further violations of Section 10 and to recover a civil penalty of up to $2,500 per violation.  
(c) In an action pursuant to this Section, a court may, in addition, do either or both of the following:  
(1) Increase the recoverable damages to an amount up to 3 times the damages otherwise recoverable under subsection (a) in cases in which the defendant has engaged in a pattern and practice of violating Section 10.  
(2) Award costs of suit and reasonable attorney's fees to a prevailing plaintiff.  
(d) The remedies provided in this Section do not preclude the seeking of remedies, including criminal remedies, under any other applicable provision of law.