Section		
28.1	Pur	pose
28.2	-	nary Users
28.3	Def	initions
28.4	Bac	kground
28.5		plicability
	A)	Social Media/Mobile Technology Safety Agreement
	<b>B</b> )	Youth in Care and Use of Social Media
	C)	Confidentiality
	D)	Images/Videos
	E)	Prohibited Use of Social Media in Child Protection Investigations
	F)	Email, Texting, Video Communications from Caseworkers
	G)	Court Orders
	H)	Criminal Acts
	I)	Cyberbullying
	J)	Sexting
	K)	Child Exploitation / Human Trafficking
	L)	Expenses from Use or Misuse of Social Media/Mobile Technology
	M)	Identity Theft
	N)	The Children's Online Privacy Protection Act ("COPPA")
Appendix	xΑ	Resources
Appendix	xВ	Criminal and Civil Laws

### Section 28.1 Purpose

The purpose of this Administrative Procedure is to provide guidance to Department (DCFS) and Purchase of Service (POS) agency staff, staff of ILO/TLP and congregate care providers, foster parents, relative caregivers, respite providers and youth in care on safe and appropriate use of the internet and social media. The Department recognizes that advances in technology have had a significant impact on everyday life.

To be effective, all primary users of this Administrative Procedure should receive ongoing training and education to ensure the protection and privacy of youth in care, persons who interact with youth in care and providers and others who interact with DCFS and POS staff. **Appendix A, Resources** contains links to resource materials that provide information useful for developing training programs and for further education. **Appendix B, Criminal and Civil Laws** contains a partial list of Illinois laws enacted to protect citizens and punish those who intentionally harm others using the internet or social media.

### **Section 28.2 Primary Users**

Primary users of this Administrative Procedure are DCFS/POS Intact Family and Permanency Workers, Supervisors, and Managers; DCFS Child Protective Services Workers, Supervisors and Managers; foster parents and unlicensed relative caregivers; staff of independent living (ILO)/transitional living (TLP) providers and congregate care providers; DCFS/POS training personnel and youth in care.

#### **Section 28.3 Definitions**

- "Caregiver" means a licensed foster parent, licensed or unlicensed relative caregiver, respite care provider, or staff of ILO/TLP and congregate care providers.
- "Caseworker" means the assigned DCFS/POS Intact Family or Permanency Worker.
- "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 of which are considered crimes and have legal consequences, including possible incarceration. (See www.kidshealth.org and **Appendix B, Criminal and Civil Laws** for more information.)
- "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 youth under 18 years of age for whom DCFS is legally responsible. This means a youth for whom DCFS has temporary protective custody, custody or guardianship via court order, or a youth whose parents have signed an adoptive surrender or voluntary placement agreement with DCFS.

### **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 Rule 431.40, Required Consents Prior to Disclosure of Personal Information.)

Likewise, criminal and civil statutes apply to digital communications. Youth 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, Criminal and Civil Laws** for a partial list of offenses.)

Illinois child welfare laws also establish the general responsibilities of the Department as a youth in care's legal custodian or guardian and define the rights and responsibilities of foster parents and relative caregivers to the youth entrusted in their care. These laws also apply to digital communication. While caregivers are not authorized to provide formal legal consents on behalf of youth in care placed in their homes, they are legally required to: maintain a safe home environment; appropriately care for and adequately supervise the children and youth in their care; handle discipline without delay; and, in accordance with DCFS policy, encourage appropriate forms of indoor and outdoor recreation. (See the Rule 340, Illinois Foster Parent Code; and Rules and Procedures 402, Licensing Standards for Foster Family Homes.)

Finally, the Children's Online Privacy Protection Act [15 U.S.C. §§6501-6506] ("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 websites, on-line 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/Mobile Technology Safety Agreement

DCFS has developed the CFS 2034, Social Media/Mobile Technology Safety Agreement 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. This Social Media/Mobile Technology Safety 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 Social Media/Mobile Technology Safety Agreement with each caregiver and each youth in care age 10 and older. The caseworker shall ask the caregiver and youth to sign the agreement if the youth will be using any social media/mobile technology. The signed agreement shall be placed in the youth's case record. 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 a youth in care is known to be using the technology at an earlier age, the Social Media/Mobile Technology Safety Agreement should be completed as soon as possible after the caseworker becomes aware of that usage.

Upon placement in a new home/setting, the caseworker shall ensure that a Social Media/Mobile Technology Safety Agreement is established between the youth and new caregiver within the first 30 days. The caseworker will review the agreement with the youth and caregiver at the caseworker's first monthly visit. The agreement shall be signed by the youth and caregiver. The signed agreement shall be placed in the youth's case record. The caseworker shall provide an extra copy of the agreement (signed or unsigned) to the caregiver and youth as a record of their agreement.

At least annually or more often as needed, the caregiver, youth, and caseworker shall:

#### **ACTION:**

Caregiver Review and sign the Social Media/Mobile Technology Safety Agreement.

Youth Review and sign the Social Media/Mobile Technology Safety Agreement.

Caseworker Review the Social Media/Mobile Technology Safety Agreement with

the caregiver and youth.

### B) Youth in Care and Use of Social Media

Youth in care may create online accounts (e.g., Facebook, Twitter, etc.) provided they meet the proper age requirements for each site. The DCFS Guardian does not support a youth in care having a social networking account if the youth is below the age required to have an account. A caregiver is not authorized to give permission in place of the DCFS Guardian.

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 as determined appropriate using normalcy parenting and the reasonable and prudent parent standard.

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.

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 Social Media/Mobile Technology Safety Agreement.

Youth

Meet with the caregiver and caseworker to read and sign the Social Media/Mobile Technology Safety Agreement.

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

Caseworker

Meet with the caregiver and caseworker to review the Social Media/Mobile Technology Safety Agreement.

Place the original signed Social Media/Mobile Technology Safety Agreement in the case record.

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 Devices**

If a youth in care brings his/her own electronic devices (e.g., tablet, MP3 player, computer or cell phone) to the caregiver's home and it is discovered that this technology is being used inappropriately, the caregiver, youth and caseworker shall:

### **ACTION:**

Caregiver Contact the caseworker about the incident(s).

Review the Social Media/Mobile Technology Safety Agreement with

the youth and the caseworker.

Youth Review the Social Media/Mobile Technology Safety Agreement with

the caregiver and the caseworker.

Caseworker Review the Social Media/Mobile Technology Safety Agreement with

the caregiver and the youth. If there is no agreement in the case record, schedule a time to meet with the caregiver and youth and

create one.

Speak to the youth about the appropriate use of the electronic

device.

If the device does not belong to the youth, attempt to locate the actual owner of the device to alert the owner of the inappropriate

use of that equipment.

### Youth in Care Using the Caregiver's Electronic Devices

If a caregiver allows a youth in care to use the caregiver's own electronic devices and the caregiver believes that this equipment is being misused, the caregiver, youth and caseworker should:

#### **ACTION:**

Caregiver Revoke the use of that device. Schedule a meeting with the

caseworker to report and discuss the misuse of the equipment.

Review the Social Media/Mobile Technology Safety Agreement with

the youth and the caseworker.

Youth Review the Social Media/Mobile Technology Safety Agreement with

the caregiver and the caseworker.

Caseworker Review the Social Media/Mobile Technology Safety Agreement with

the caregiver and the youth. If there is no agreement in the case record, schedule a time to meet with the caregiver and youth and

create one.

Speak to the 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

When confidential information is disseminated over any social media or mobile technology, all control of that information is lost.

The following types of private/personal information should never be shared on 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/personal 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 care 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 email 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 the youth as a "foster child" or 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 youth in care in any form, including any posted online images, should not identify those youth as "foster children" or youth in care.

The DCFS Guardian must consent, in advance, to the release of any image or picture of a youth in care if that youth is going to be identified as a "foster child" or 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 shall be embedded within the photo. Since identification of the location may constitute a violation of confidentiality, it is recommended that youth in care 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, youth in care, and caseworkers shall:

### **ACTION:**

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

## E) Prohibited Use of Social Media in Child Protection Investigations

While offering some additional avenues for making some contacts, social media contacts do not replace any required in-person contacts in child protection investigations. Child Protection Specialists shall not use social media to meet any in-person mandate in Procedures 300.

Child Protection Specialists are required to make good faith attempts to establish in-person contact with alleged child victims and all subjects of a report. "Good faith attempt" is defined in **Procedures 300.15**, **Definitions** as "a diligent and honest effort to make in-person contact with an alleged child victim and all subjects of a report." Contact via social media is not an acceptable substitute for in-person contact with the involved child/children or subjects of a report.

Child Protection Specialists must also comply with all instructions regarding in-person interviews in Procedures 300. Appendix B(h), Contacts, Activities, and Documentation Required for ALL Allegations.

## F) Email, Texting, or Video Communications from Caseworkers

A caseworker shall not share personal information of persons served by DCFS using any State-owned device, or using DCFS-approved social media/mobile technology downloaded on a State-owned device, for any non-work related purpose.

A caseworker shall not share personal information of persons served by DCFS using any <u>personal</u> device, or using DCFS-approved social media/mobile technology downloaded on a personal device, for any non-work related purpose.

Caseworker contact with youth in care or DCFS clients for a non-work related purpose is strictly prohibited, whether the caseworker is using a State-owned or personal device or DCFS-approved or personal social media/mobile technology,

- Email. Caseworkers may transmit personal information of persons served by the Department via DCFS Outlook email to a non-DCFS Outlook email address only when sending the information through a Department- or State of Illinois-authorized secure transmission. All transmissions by authorized users must be made in accordance with Rules and Procedures 431, Administrative Procedure #20, the Social Work Code of Ethics and current law.
- **Texting.** It is permissible to contact a youth in care, caregiver or DCFS client via 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 caseworkers to use video communications (e.g., Skype, FaceTime, Web Ex, etc.) or similar applications to interact with a youth in care, caregiver or client. These types of video communications are the equivalent of a phone contact. Video communications do not replace in-person contacts required by Procedures 315.130, Worker Contacts and Interventions, Procedures 302.388, Intact Family Services, or other DCFS policies, but can offer opportunities for additional visual contacts with youth in care, caregivers and DCFS clients.

If there are suspected inappropriate communications by the caseworker, the caregiver, youth, and caseworker/supervisor shall:

#### **ACTION:**

Caregiver Notify the assigned caseworker/supervisor.

Youth Notify the assigned caseworker/supervisor.

Caseworker/ Contact the Regional DCFS Office of Legal Services.

Supervisor

### **G)** Court Orders

All court orders that prohibit certain contact, or 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 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.

### H) 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. **Appendix B, Criminal and Civil Laws** contains a partial list of Illinois laws enacted to protect citizens and punish those who intentionally harm others using the internet or social media. 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 or 800-964-3013 (TTY)

Fax: 312-814-8283 100 W Randolph

12th Floor

Illinois Attorney General High Tech Crimes Bureau

Chicago, IL. 60601

### I) 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 youth receives mean or threatening e-mail messages, text messages, or instant messages;
- Someone has posted mean or hurtful things about a youth online;
- Someone has forwarded a youth's e-mails or text messages to another person without the youth's permission;
- Someone has altered a picture of a youth online;
- Someone has taken pictures of a youth without the youth's permission and posted the picture(s) online;

- Someone has stolen a youth's password and is sending messages, posting information or pretending to be the youth; or
- 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 Social Media/Mobile Technology Safety Agreement, with

the youth and caseworker.

Report improper content and usage to the perpetrator's websites or internet Service Provider (ISP). (Most websites and ISPs have a service agreement that prohibits members from using their service to harass or threaten others. Most websites and ISPs 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.

 $Review \ the \ Social \ Media/Mobile \ Technology \ Safety \ Agreement \ with$ 

the youth and caregiver.

Report improper content and usage to the perpetrator's website or ISP. Most websites and ISPs have a service agreement that prohibits members from using their service to harass or threaten others. Most websites and ISPs also supply a link to report this type

of abuse.

Caregiver, If you believe any person is being bullied online, call 1-888-414-

Youth, or 7678 or email e-info@atg.state.il.us to contact an Internet Safety

Caseworker: Specialist at the Illinois Attorney General's Office.

### J) 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 youth in care under 18 years of age who sends, requests or receives indecent photos using a cell phone, tablet, portable or mobile computer or other device could be put under the supervision of the Juvenile Justice Division through Juvenile Court. The youth could be ordered to obtain counseling or other supportive services to address the situation and also be ordered to perform community service. The youth could also be criminally prosecuted. Section 3-40(e) of the Juvenile Court Act of 1987 specifically states:

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. [705 ILCS 405/3-40(e)]

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

#### **ACTION:**

Caregivers Contact the caseworker.

Review the Social Media/Mobile Technology Safety Agreement with the youth and caseworker

the youth and caseworker.

If you allow a youth in care 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 Social Media/Mobile Technology Safety Agreement with

the caregiver and the caseworker.

Caseworker Review the Social Media/Mobile Technology Safety Agreement

with the caregiver and the youth.

Contact the Regional DCFS Office of Legal Services.

### K) 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, predators often make their first contact with their child 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 the youth 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 the youth might be engaged by a trafficker via social media. For more information about the prevention, identification, and response to human trafficking, see **Procedures 302.Appendix C, Human Trafficking** 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 Social Media/Mobile Technology 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 Social Media/Mobile Technology 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: internet Crimes Against Children (ICAC) Taskforce

Illinois Crimes Against Children Taskforce Office: 312-814-3762 or 800-964-3013 (TTY)

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 **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.

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

Neither the Department nor the DCFS Guardian is financially or legally responsible for any costs associated with a youth's wireless communications that violate existing laws or occur as a result of any act, error, submission or omission by a youth's foster parent, relative caregiver or other provider (See Administrative Procedure #13, Foster Child Damage Reimbursement Program.)

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 how to submit a claim

for reimbursement under DCFS Administrative Procedure 13,

Foster Child Damage Reimbursement Program.

Youth Review the Social Media/Mobile Technology Safety Agreement with

the caregiver and the caseworker.

Caseworker Review the Social Media/Mobile Technology Safety Agreement with

the caregiver and the youth.

## M) 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:

866-999-5630 or 877-844-5461 (TTY).

Youth Talk to your caregiver and caseworker.

Caseworker Meet with the caregiver and youth to review the circumstances of

the possible identity theft.

Call the toll-free Illinois Attorney General Identity Theft Hotline at:

866-999-5630 or 877-844-5461 (TTY); and

Contact the Office of the DCFS Guardian immediately by Outlook

email at DCFS. CreditChecks or by phone at 312-814-8600.

## N) The Children's Online Privacy Protection Act ("COPPA")

"COPPA" (is a federal law 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 Guardian about taking action to protect a youth's

information.

This page intentionally left blank.

### APPENDIX A – RESOURCES

**Training.** DCFS offers on-demand pre-service and in-service training for caseworker staff and caregivers on its Virtual Training Center (VTC) website, including courses on social media mobile technology safety.

#### **On-line Websites and Resources:**

- www.onguardonline.gov: This federal government website is dedicated to teaching online safety, security, and responsibility.
- www.netsmartz.org: NetSmartz Workshop is an interactive, educational program offered by the National Center for Missing and Exploited Children (NCMEC) that provides age-appropriate resources to help teach children how to be safer on- and offline.
- http://www.missingkids.com: This is the website for the National Center for Missing and Exploited Children.
- www.wiredsafety.org: WiredSafety is an online safety, education, and help group.
- <u>www.fosi.org/good-digital-parenting</u>: Tips and resources for parents from the Family Online Safety Institute.
- <u>www.healthychildren.org</u>: Internet safety guidelines created by The American Academy of Pediatrics.

### 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 **800-843-5678** (toll-free) to report crimes against children, including online enticement of children for sexual acts, obscene material sent to a child, and child pornography. The CyberTipline is funded by the National Center for Missing and Exploited Children (NCMEC).

### **Cyberbullying Websites**

- www.brainpop.com/technology/communications/cyberbullying/
- www.cyberbully411.org
- www.commonsensemedia.org/cyberbullying
- http://kidshealth.org/parent/positive/talk/cyberbullying.html

## Websites for Kids and Teens

- www.netsmartzkids.org: internet safety games for children 5-10 years of age.
- www.nsteens.org: This is a NetSmartz site that teaches tweens and teens about making safer choices online.

### **Search Engines for Children**

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

### Identity Theft: Contact the Attorney General's Office Illinois Identity Theft Hotline

Identity theft occurs when someone uses another person's personal information (e.g., name, Social Security number, or bank account number) without that person's knowledge to commit fraud or theft.

The Illinois Identity Theft Hotline provides Illinoisans who have (or believe they 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.

- Identity Theft Hotline (toll-free): 866-999-5630 (toll-free) or TTY: 877-844-5461.
- Identity Theft Hotline Brochure (available in English, Spanish and Polish)
- https://illinoisattorneygeneral.gov/consumers/Identity\_Theft\_Resource\_Guide.pdf

### Illinois Attorney General's Website (www.illinoisattorneygeneral.gov)

In addition to identify theft, the Attorney General's website provides information regarding credit reporting, credit disputation and online scams.

The website also provides phone numbers and internet links to report child exploitation and pornography:

- Illinois Child Exploitation Task Force: Phone: 312-814-3762, TTY: 800-964-3013.
- 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.

### National Center for Missing and Exploited Children (NCMEC)

NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet.

Contact the CyberTipline: **800-843-5678** (toll-free) or via the NCMEC's website: www.missingkids.org/gethelpnow/cybertipline.

#### **Contact Information**

Illinois Crimes Against Children Taskforce (ICAC) High Tech Crimes Bureau 100 W Randolph, 12th Floor Chicago, IL. 60601

Office: **312-814-3762** Fax: **312-814-8283** 

### APPENDIX B - CRIMINAL AND 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**

NAME	Harassment through Electronic Communications
CITATION	§26.5-3(a) of the Illinois Criminal Code [720 ILCS 5/26.5-3]
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.
CONSEQUENCE	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.  A person who violates this law is guilty of Class B misdemeanor.
CONSEQUENCE	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 years 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.

NAME	Stalking
CITATION	§12-7.3 of the Illinois Criminal Code, [720 ILCS 5/12-7.3]
SUMMARY	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.
CONSEQUENCE	Stalking is a Class 4 felony; a second or subsequent conviction is a Class 3 felony.

NAME	Cyber Stalking
CITATION	§12-7.5 of the Illinois Criminal Code, 720 ILCS 5/12-7.5]
SUMMARY	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 emotion 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, surreptitiously, and without lawful justification, installs or otherwise places electronic monitoring software or spyware on an electronic communication device as a means to harass another person and: 1) at any time transmits a threat 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) places that person or a family member of that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint; or at any time knowingly solicits the commission of an act by any person which would be a violation of this Code directed towards that person or a family member of that person.
	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.
CONSEQUENCE	First offense is Class 4 felony; second and subsequent conviction is Class 3 felony.

NAME	Minors Involved in Electronic Dissemination of Indecent Visual Depictions
	in Need of Supervision
CITATION	§3-40 of the Juvenile Court Act of 1987 [705 ILCS 405/3-40]
SUMMARY	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.
CONSEQUENCE	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.

NAME	Hate Crime
CITATION	§12-7.1 of the Illinois Criminal Code [720 ILCS 5/12-7.1]
SUMMARY	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, Intimidation, Stalking, Cyberstalking, Misdemeanor Theft, Criminal Trespass To Residence, Real Property, Or Vehicle, Misdemeanor Criminal Damage To Property, Mob Action, Disorderly Conduct, Harassment By Phone, or Harassment Through Electronic Communications.
CONSEQUENCE	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.

NAME	False Personation; Solicitation
CITATION	§17.2 of the Illinois Criminal Code [720 ILCS 5/17-2]
SUMMARY	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, injury, 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.
CONSEQUENCE	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.

NAME	Internet Offenses
CITATION	§16-40 of the Illinois Criminal Code [720 ILCS 5/16-40]
SUMMARY	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.
CONSEQUENCE	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.

NAME	Unauthorized Video Recording and Live Video Transmission
CITATION	§26-4(a) of the Illinois Criminal Code [720 ILCS 5/26-4(a)]
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:
	<ul> <li>in a restroom, tanning bed, tanning salon, locker room, changing room, or hotel bedroom.</li> </ul>
	• 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.
	<ul> <li>under or through the clothing worn by that person for the purpose of viewing the body or the undergarments worn by that person.</li> </ul>
	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.

NAME	Harassing and Obscene Communications
CITATION	§26-4(a) of the Illinois Criminal Code [720 ILCS 5/26-5]
SUMMARY	A person commits transmission of obscene messages when he or she sends messages or uses language or terms which are <b>obscene</b> , <b>lewd or immoral with the intent to offend</b> 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	Sentencing for violations range from Class B misdemeanor, Class 4 felony. The court may order any person convicted under this Article to submit to a psychiatric examination.

NAME	Harmful Material
CITATION	§11-21 of the Illinois Criminal Code [720 ILCS 11-21]
SUMMARY	A person is guilty of distributing harmful material to a minor when he or she:
	• Knowingly sells, lends, distributes, exhibits to, depicts to, or gives away to a minor, knowing that the minor is under the age of 18 or failing to exercise reasonable care in ascertaining the person's age:
	<ul> <li>Any material which depicts nudity, sexual conduct, or sado-masochistic abuse, or which contains explicit or detailed verbal descriptions or narrative accounts of sexual excitement, sexual conduct or sado- masochistic abuse, and which taken as a whole is harmful to minors:</li> </ul>
	<ul> <li>A motion picture, show, or other presentation which depicts nudity, sexual conduct or sado-masochistic abuse and is harmful to minors: or</li> </ul>
	<ul> <li>An admission ticket or pass to premises where there is exhibited or to be exhibited such a motion picture, show, or other presentation; or</li> </ul>
	<ul> <li>Admits a minor to premises where there is exhibited or to be exhibited such a motion picture, show, or other presentation, knowing that the minor is a person under the age of 18 or failing to exercise reasonable care in ascertaining the person's true age.</li> </ul>
CONSEQUENCE	Distribution of harmful material in violation of this Section is a Class A misdemeanor. A second or subsequent offense is a Class 4 felony.
	Any person under the age of 18 who falsely states, either orally or in writing, that he or she is not under the age of 18 (is an adult), or who presents or offers to any person any false identification evidence or not actually his or her own in order to order, obtain, view, or otherwise procure or attempt to view any harmful material is guilty of a Class B misdemeanor.
	A person over the age of 18 who fails to exercise reasonable care in ascertaining the true age of a minor, knowingly distributes, or sends, or causes to be sent, or exhibits to, or offers to distribute, or exhibits any harmful material to a person that he or she believes is a minor is guilty of a Class A misdemeanor. If that person used a computer web camera, cell phone, or any other type of device to make the harmful material, then each offense is a Class 4 felony.

## **CIVIL STATE LAWS**

NAME	Suspension or Expulsion of Pupils; School Searches
CITATION	§10-22.6 of the Illinois School Code [105 ILCS 5/10-22.6]
SUMMARY	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.
CONSEQUENCE	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. In school-suspensions programs permitted.

NAME	Electronic Paging Devices on School Property (Cities over 500,000)
CITATION	§34-18.9 of the Illinois School Code [105 ILCS 5/34-18.9]
SUMMARY	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.
	<ul> <li>(c) The Board of Education shall develop and circulate written standards to each principal, under which a principal:</li> <li>(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 (2) may impose appropriate discipline or other sanctions against any student who violates any provision of this Section.</li> </ul>
CONSEQUENCE	Principal may impose appropriate discipline or other sanctions against any student who violates this provision.

NAME	Transportation Vehicle Communication Devices
CITATION	§12-610.2 Electronic communication devices. [625 ILCS 5/12-610.2]
SUMMARY	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:
	<ul> <li>Driver using electronic communication device for the sole purpose of reporting an emergency situation and continued communication with emergency personnel during the emergency situation;</li> </ul>
	<ul> <li>A driver using an electronic communication device in hands-free or voice operated mode, which may include the use of a headset;</li> </ul>
	<ul> <li>A driver using an electronic communication device whole parked on the shoulder of a roadway;</li> </ul>
	A driver using an electronic communication device by pressing a single button to initiate or terminate a voice communication; or
	<ul> <li>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.</li> </ul>
CONSEQUENCE	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.

NAME	Anti-Phishing Act
CITATION	§10 of the Illinois Civil Liabilities Code [740 ILCS 7/10]
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.
	<ul><li>(2) Award costs of suit and reasonable attorney's fees to a prevailing plaintiff.</li><li>(d) The remedies provided in this Section do not preclude the seeking of remedies, including criminal remedies, under any other applicable provision of law.</li></ul>

This page intentionally left blank.