STATE OF ILLINOIS
ILLINOIS STATE POLICE
LAW ENFORCEMENT PORTAL

USER AGREEMENT FOR SCHOOL ADMINSTRATORS

This agreement is entered into by and between:

_____*(Participating Agency)* and the Illinois State Police (hereinafter referred to as ISP). The Agreement sets forth the conditions governing the Participating Agency's use of ISP's Law Enforcement Portal for the purposes of submitting clear and present danger reports.

RECITALS

WHEREAS, The ISP maintains and operates the Law Enforcement Portal; and

WHEREAS, The Participating Agency is a governmental entity with statutory authority to submit clear and present danger reports; and

WHEREAS, this User Agreement is authorized pursuant to the provisions of Article 7, Section 10 of the Illinois Constitution and the Intergovernmental Cooperation Act [5 ILCS 220].

NOW, THEREFORE, ISP and Participating Agency agree as follows:

ARTICLE I: DEFINITIONS

School Administrator Definition and Duties— It is the duty of the principal of a public elementary school or secondary school, or his or her designee, and the chief administrative officer of a private elementary or secondary school or a public or private community college, college, or university, or his or her designee, to report to the Illinois State Police when a student is determined to pose a clear and present danger to himself, herself, or to others, within 24 hours of the determination. [430 ILCS 65/8.1(d)(2) and 430 ILCS 66/105]

Participating Agency— The Participating Agency is any governmental entity or individuals employed by that entity, as defined in Article I of this Agreement.

Clear and Present Danger— Clear and present danger means a person "demonstrates threatening physical or verbal behavior, such as violent, suicidal, or assaultive threats, actions, or other behavior, as determined by a physician, clinical psychologist, qualified examiner, school administrator, or law enforcement official." (430 ILCS 65/1.1).

ARTICLE II: PURPOSE AND AUTHORITY

The purpose of this User Agreement is to provide the Participating Agency an electronic means to

report when he or she has determined that a person poses a clear and present danger. If a person is determined to pose a clear and present danger to himself, herself, or to others, school administrators shall notify the ISP within 24 hours of making the determination. (430 ILCS 65/8.1(d)(2)). This Agreement is intended to enhance and foster the responsible exchange of information by ensuring that the Participating Agency and the ISP understand their respective roles and responsibilities.

ARTICLE III: ASSUMPTION OF RISKS AND INDEMNIFICATION

The Participating Agency is responsible for verifying the quality and accuracy of the information submitted. The ISP has no liability to the Participating Agency or its designees for any damages (including but not limited to special, incidental, direct, indirect, punitive, or consequential) arising from the use of the ISP's Law Enforcement Portal. By entering into this Agreement, the Participating Agency and its designees agree to assume, without limitation, all risks of loss and indemnify and hold harmless ISP and any of its agents/employees against any and all claims, actions, losses, expenses, and damages that may arise from the Participating Agency's submission of Clear and Present Danger Determinations. Nothing in this Agreement is intended to create a private right of action for any member of the public or alter existing or future federal and state law requirements. A waiver of any condition of this Agreement must be requested in writing. No waiver of any condition of this Agreement may be effective unless in writing and signed by the ISP and the Participating Agency.

ARTICLE IV: RESPONSIBILITIES

Participating Agency's Responsibilities:

a. The Participating Agency is responsible for any and all Clear and Present Danger Determinations submitted through the portal by any of its users.

b. The Participating Agency shall ensure that he or she understands the requirements for Clear and Present Danger Determinations, is authorized for system access, and follows all requirements within this Agreement.

ARTICLE V: MAINTENANCE OF RECORDS

a. The ISP shall maintain and be the custodian of all records pertaining to clear and present danger reporting. The ISP shall maintain all records in compliance with relevant Record Retention Schedules and the State Records Act. [5 ILCS 160/et seq.]

b. The Participating Agency shall not take screenshots, print, or make copies of any clear and present danger reporting submitted through the ISP Law Enforcement Portal.

ARTICLE VI: DURATION, MODIFICATION, AND TERMINATION

a. This Agreement shall be in effect upon the signature of the Director of the Illinois State Police, or a properly appointed designee. The Agreement will be in effect for one year from the final date of signature and shall renew automatically for one-year periods. Each party shall review the Agreement prior to the annual renewal date.

b. Modifications to this Agreement may be made, but only in writing and signed by both parties.

c. This Agreement will terminate when either party notifies the other of its intent to discontinue the Agreement. Notice shall be provided to the parties listed in Article XI of this Agreement. The terminating party will provide the other party written notice at least 30 days prior to the desired termination date.

ARTICLE VII: USE OF PORTAL

a. The ISP shall permit the Participating Agency limited access to the ISP Law Enforcement Portal and shall provide the Participating Agency one (1) username for purposes of submitting a clear and present danger report as defined in Section 1.1 of the Firearm Owners Identification Card Act. [430 ILCS 65/1.1(13)]

ARTICLE VIII: FREEDOM OF INFORMATION ACT

a. In its afore-mentioned role as the custodian of all records generated, the ISP shall respond to requests for records made under the Freedom of Information Act (FOIA). [5 ILCS 140/et seq.]

b. The Participating Agency is responsible for serving as the custodian of its records and responding to requests made to it under the Freedom of Information Act. [5 ILCS 140/et seq.]

ARTICLE IX: INFORMATION SECURITY PROTOCOLS

Should a security breach result in unauthorized acquisition of personal information, information owners will be notified of the incident in a timely manner, in accordance with the Personal Information Protection Act. (815 ILCS 530/1 *et seq*.). The Participating Agency shall immediately notify the ISP's upon discovery of a breach of the system or system data. The Participating Agency shall have 90 days to report to the ISP what steps have been taken to protect the information from future compromise. ISP shall notify the Participating Agency if information or data has been improperly disclosed. Once the nature of the breach has been determined, the ISP will work with the Participating Agency to facilitate proper notification to affected individuals in accordance with the Personal Information Protection Act. Personal information is defined as an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social Security number;

(2) Driver's license number or state identification card number;

(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account

(4) Medical Information;

(5) Health Insurance Information; or

(6) Unique Biometric Data generated from measurements or technical analysis of human body characteristics used by

the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Personal information will be considered to be acquired, or reasonably believed to be acquired, by an unauthorized person in any of the following situations:

(1) Loss of documents – lost or stolen documents containing personal information.

(2) Loss of computing system – Loss of any server, desktop, laptop, or personal digital assistant (PDA) containing unencrypted personal information.

(3) Hacking incident – A successful intrusion of a computer system via the network.

(4) Unauthorized data access – The access or attempt to access data by individuals who are unauthorized to access that data. This includes situations where individuals have received data that they are unauthorized to access: emails sent to the wrong recipient, paper documents sent to the wrong recipient and incorrect computer access settings. This also covers situations where unencrypted personal information has been downloaded, copied or used by an unauthorized person.

ARTICLE X. SUSPENSION/TERMINATION OF SERVICE

ISP reserves the right to immediately and unilaterally suspend or terminate the Participating Agency's access to the Portal when any term of this Agreement is violated. If this agreement is terminated, the Participating Agency will still have an obligation to report Clear and Present Danger Determinations as required by applicable state law. Suspended service shall only be resumed upon such terms and conditions as the ISP shall deem appropriate under the circumstances. Suspension may be followed by termination if deemed necessary by ISP.

ARTICLE XI: NOTICES

All required notices shall be delivered to the following:

To the Participating Agency:

Name:

Title:

Agency:

Address:

To the ISP:

Name: Office of Firearms Safety
Title: Firearms Safety Counsel
Elizabeth Leahy
Address: 801 South 7th St. 600S,
Springfield, Illinois 62703

_____ _____

Participating Agency Date

_____ _____

Director of the Illinois State Police Date