ILLINOIS ASSOCIATION OF SCHOOL BOARDS

Office of General Counsel

Could a Freedom of Information Act (FOIA) Request be *Phishing*?

June 2018

IASB publishes this guidance as part of its continuing effort to provide assistance to school leaders. Potential questions may arise that are not addressed in this guidance. **This guidance is published for informational purposes only, and is not a substitute for legal advice. For legal advice or a legal opinion on a specific question, you should consult a lawyer.**

1. **We received a suspicious-looking FOIA request via e-mail and believe the requestor may be *phishing* – trying to fraudulently obtain financial or other confidential information by masquerading as a reputable entity or person. Do we have to respond to this FOIA request?**

   Yes. FOIA requires that all public bodies promptly respond to FOIA requests within five business days after receipt of the request, unless the time for response is extended. 5 ILCS 140/3(d). A response is required regardless of who/where the FOIA request comes from.

2. **Can we respond to the suspected FOIA *phishing* request by explaining that we believe the requestor is *phishing* and then denying the requested records in their entirety?**

   No. The legal bases for denying a FOIA request (either partially or in its entirety) do not include denial based upon suspected *phishing*. However, school districts may deny requested records that fall within one of FOIA's many exemptions. 5 ILCS 140/7 and 140/7.5.

   Before responding to a FOIA request from a suspected *phisher*, districts should review the request with their board attorney to confirm that the records requested fall within the FOIA definition of "public records." 5 ILCS 140/2(c). If they do, then the board attorney should ensure that all available exemptions are asserted and that exempt portion(s) of requested records containing both exempt and non-exempt material is redacted.

3. **What types of exempt information do FOIA *phishers* often request?**

   FOIA phishers often request information that can be used to perpetuate identity theft or fraud, such as: social security numbers, employee identification numbers, personal financial information, home/personal telephone numbers, and personal email addresses. All of these items are "private information" exempt from disclosure under FOIA. 5 ILCS 140/2(c-5) and 140/7(1)(b). FOIA phishers may also request birthdates, which may be exempt from disclosure as "personal information…the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 ILCS 140/7(c)

4. **Is there anything we can do to combat suspected *phishing* via FOIA requests?**

   If your district receives a suspected FOIA *phishing* request, first contact your board attorney. Then, consider working with your board attorney and district information technology staff to try to identify the source of the suspected FOIA *phishing* request, for example by verifying the Internet Protocol address of an electronic FOIA request. This may help you determine if the FOIA request actually is a *phishing* attempt. Regardless of your investigation results, however, please remember that the law requires you to respond to the FOIA request. *See* No. 1, above.

Prepared by: **Maryam T. Brotine**, IASB Assistant General Counsel