NEW GUIDELINE - TECHNOLOGY UPDATE

NOTIFICATION INFORMATION SECURITY INCIDENT

As required by AG 8305B, if a user, who has access to District Confidential Data/Information and/or to any mission-critical system, suspects that there may have been an information security incident, the user must promptly report the incident to a District administrator who shall immediately notify the Superintendent and the District's Information Technology Office and/or Security Office.

If an information security incident occurs that involves the release of District Confidential Data/Information, the District will take action in accordance with State and Federal law to address the situation, including, when appropriate and/or legally required, notifying affected individuals that their personally-identifiable information was improperly accessed and/or released. Any required notices will be provided in a timely manner.

Pursuant to State law, the District shall disclose any security breach of computerized personal information data ("breach of the security of the system"), following its discovery or notification of the breach of the security of the system, to any Ohio resident whose personal information (as defined below) was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

For purposes of this policy, "breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by the Board of Education and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of an Ohio resident.

"System" means any collection or group of related records that are kept in an organized manner, that are maintained by the District, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

"Personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one (1) or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (a) social security number; (b) driver's license number or State identification card number; or (c) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

The notice to individuals required by State law shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the District to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than forty-five (45) days after the discovery or notification of a breach, unless subject to an authorized delay.

If a Federal, State, or local law enforcement agency determines that disclosure or notification to individuals required under this guideline would impede a criminal investigation, or jeopardize homeland or national security, the notice shall be delayed until the law enforcement agency determines the disclosure or notification will not compromise the investigation or jeopardize homeland or national security.

[ ] Notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant Federal, State, or local law enforcement agencies, the District reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm or fraud to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least _____ **[e.g., five (5)]** years.

The District will make the State-mandated disclosure or notification by one (1) of the following methods:

A. written notice

B. electronic notice, if the District's primary method of communication with the resident is by electronic means

C. telephone notice

The District may provide substitute notice in lieu of direct notice if (a) the District does not have sufficient contact information to provide notice in one (1) of the manners described above, (b) the cost of providing disclosure or notice would exceed $250,000, or (c) the affected class of residents exceed 500,000 persons. Such substitute notice shall include all of the following:

A. electronic mail notice if the District has an e-mail address for the resident

B. a conspicuous posting of the disclosure or notice on the District's website

C. notification to major media outlets (including print and broadcast) to the extent the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equal seventy-five percent (75%) of the State's population

If the District discovers circumstances that require State-mandated disclosure pursuant to this guideline to more than 1,000 residents involved in a single occurrence of a breach of the security of the system, the District shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the District to affected Ohio residents.

In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the District of the breach of security as expeditiously as practicable, but no later than _____ **[e.g., ten (10)]** days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, the District shall provide the notices required above. A third-party agent shall provide the District with all information that the District needs to comply with its notice requirements.

An agent, pursuant to a contract entered into by the District prior to the date of the breach of the security of the system occurred, may provide notice as required on behalf of the District, so long as the contract does not conflict with any provision of R.C. 1347.12.

R.C. 1347.12, 1349.191, 1349.192
FERPA