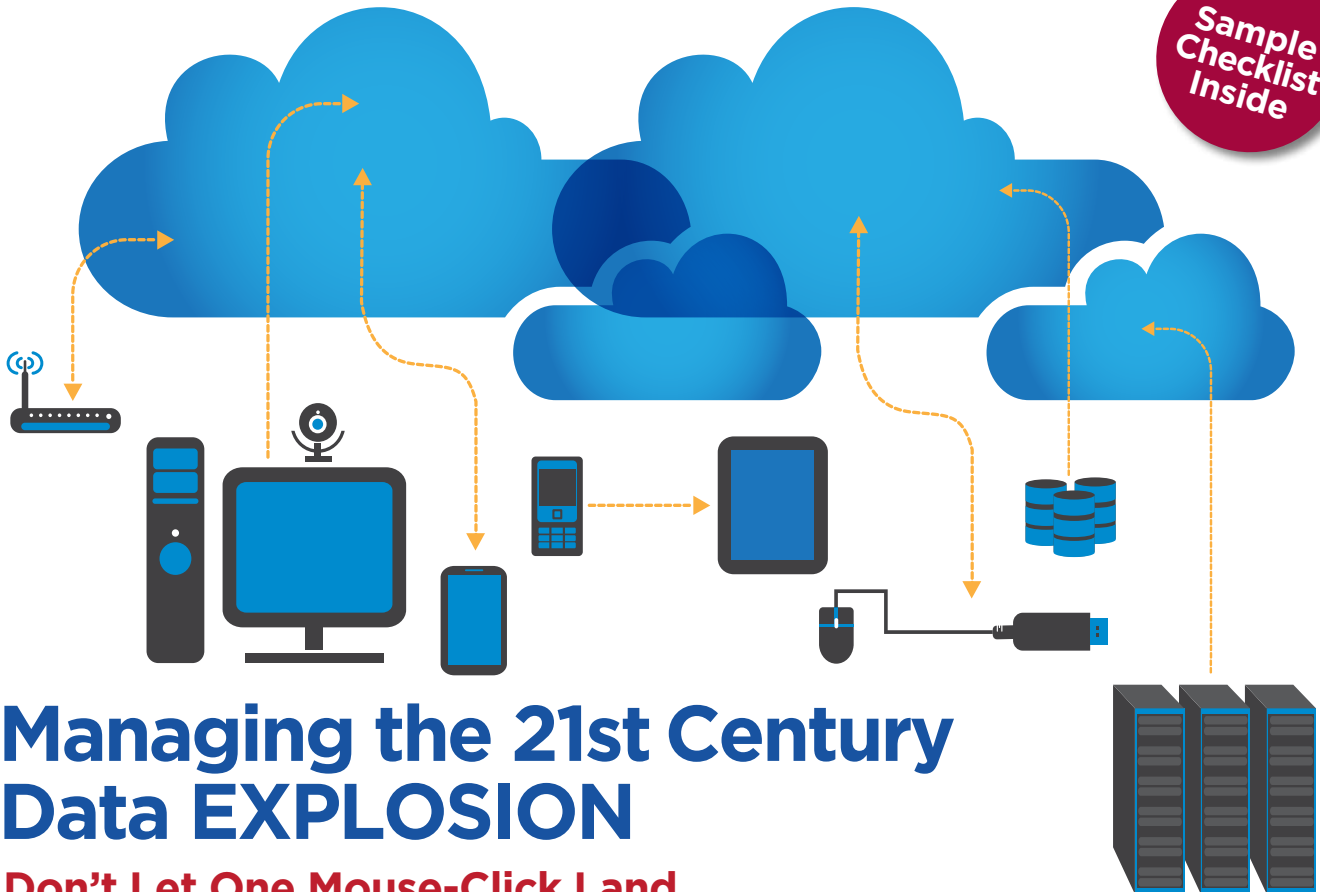**Sample Checklist Inside**

Managing the 21st Century Data EXPLOSION

Don't Let One Mouse-Click Land Your District in Hot Water

Like most organizations across the nation, school districts face a significant challenge in properly managing Electronically Stored Information ("ESI"). What is ESI? It is the overwhelming amount of electronic data captured by servers; hard drives; instant messaging programs; smart phones, watches and other devices; tablets; apps; websites; server logs; and many other data recording devices. This data includes both the information that users knowingly save and the vast amount of electronic information that is created and saved without most users even realizing it. In addition, the proliferation of technology has changed the way people work, creating new challenges to locating and retaining data. Text messaging, social media, and cloud-based "educational

technology" resources are frequently used as work tools – yet many users do not understand how or why data created from these tools may need to be saved.

Electronic data could eventually serve as critical evidence should your district ever be faced with litigation. Moreover, failure to handle electronic data properly and consistently before litigation arises can lead to crippling costs after a lawsuit has been filed.

We at SLRMA know that implementing and following ESI policies are a critically important part of risk management for school districts. That is why SLRMA is proud to bring to our members the Electronic Data Self-Audit Checklist 2016, specifically designed with school districts in mind.

Checklist Excerpt

Electronic Data Self-Audit Checklist for School District Employers, 2016 Update

MANAGEMENT OF ELECTRONICALLY STORED INFORMATION
OUTSIDE THE LITIGATION CONTEXT

A. Appropriate Use of The District's Email and Other Computer Systems

    1. Email Policies

The most important message that a district email policy should convey to employers and other users is to think twice before they hit the "send" button. In certain contexts, it may be more appropriate for a user to have a conversation over the phone or in person, especially if he or she wishes to express personal opinions or criticize others. It might be helpful for the district to advise users of a general rule of thumb: "If a local newspaper printed your email on its front page, would it cause embarrassment or have other adverse consequences for you or the district?"

- Does the District have a written policy on use of email? ☐ Yes ☐ No

If the District has such a policy:

- Has the policy been approved by the appropriate authority/governing body? ☐ Yes ☐ No
- Has the policy been reviewed by legal counsel for compliance with applicable local, state, and federal law? ☐ Yes ☐ No
- Is the policy accessible to users of the district's email system? ☐ Yes ☐ No
- Are users required to provide written confirmation that they have read and agree to abide by the policy? ☐ Yes ☐ No
- Does the policy contain provisions that:
    - Describe acceptable and unacceptable uses of email and the consequences for failure to comply with the policy? ☐ Yes ☐ No
    - Inform users that by using the district's email system they waive any right to privacy in any email they create, send, receive, or store in the system? ☐ Yes ☐ No
    - Place users on notice that the district can and may monitor users' email without prior notification? ☐ Yes ☐ No
    - Require users to report any incidents of email abuse to their managers and/or the IT Department? ☐ Yes ☐ No
    - Establish that the district's email system is to be used primarily for district business? ☐ Yes ☐ No
    - Restrict personal use that is unreasonable, irresponsible, interferes with district business, or is contrary to law? ☐ Yes ☐ No
    - Prohibit encryption of email without prior written permission from supervisors and/or the IT Department? ☐ Yes ☐ No
    - Prohibit users from using another user's email account or permitting another user to use their account? ☐ Yes ☐ No

This is a portion of the Electronic Data Self-Audit Checklist for School District Employers, 2016 Update.

Download the complete checklist at SLRMA.org

Is my school district required to save every email or draft document ever created?

Absolutely not! The decision to save a given email or document will depend on many factors, including the existence of a litigation hold, any regulatory requirements, any digital storage space, and the importance of the communication.

Does having an ESI policy mean that everything my school district does has to be in writing?

No, not at all. Districts may want to explain specific protocols for when email, as opposed to a telephone call, is appropriate to avoid potential embarrassment to, or other adverse consequences for, the employee or the district.

Recent Dispatches in the Newsroom

NEW Federal Cases

October 2016

Ziegler v. Martin County School District

The Federal 11th Circuit Court of Appeals issued an opinion on a case in which students were denied admission to Prom. Read this interesting case in preparation for the upcoming school dance season and learn how school officials handled suspected student alcohol consumption when a large group of students arrived at their prom on a "party bus."

December 2016

Brinsdon v. McAllen Independent School District

In late 2016, the Federal 5th Circuit Court of Appeals ruled on a matter in which a Texas high school student took issue with an assignment in her Spanish class. Read the Court's findings in this unusual case that gathered national media attention prior to suit being filed.

School districts may want to include the district's retention policies in employee handbooks, and require employees to sign an acknowledgement of receipt. Employee training on specific issues may also be appropriate. At a minimum, employees should be clearly aware of ESI protocol.

How can the SLRMA Electronic Data Self-Audit Checklist help?

The Self-Audit Checklist assists school districts in managing their ESI and consists of two parts. Part I focuses on inventory and retention policies, including important considerations for designing an effective retention policy. Part II addresses ESI management for potential litigation, during litigation, and after litigation has concluded.

We encourage SLRMA members to relook at their current data preservation policies and proactively manage their ESI. A consistently applied retention policy and properly applied "hold" in the face of a credible threat of imminent litigation is the best way to avoid the costs of data restoration, or worse, court sanctions, which may accompany electronic discovery demands. Retention and deletion policies should be routinely tested and revised to address changes in technology or legal risks. Although consultation with local counsel may be needed to rework outdated policies and procedures, or when litigation is looming, using this Self-Audit Checklist will point your district toward a better understanding and a consistent approach in managing data.

Maree F. Sneed
Partner
Hogan Lovells
US, LLP
(Washington, D.C.)

Dr. Troy Loeffelholz
Superintendent
Columbus Public
Schools
(Columbus, NE)

Cheryl L. Sandner
President
Brokers' Risk
(Chicago, IL)

Dr. Jerry D. Weast
CEO
Partnership for
Deliberate
Excellence, LLC
(Potomac, MD)

Dr. Joe Siano
Superintendent
Norman Public
Schools
(Norman, OK)

Tracy L. Olsen
SLRMA Chief Content Editor
Senior Managing Counsel,
Brokers' Risk
(Chicago, IL)

Dr. Gillian Chapman
Superintendent
Teton County
School District
(Jackson, WY)

Ivy League Support
A New Approach to Anti-Bullying

Interested in innovative approaches to reduce bullying, and thereby manage your school district's risks more effectively? Researchers from Princeton, Rutgers and Yale have produced a curriculum that harnesses the power of "student influencers" - and it's free to all interested.

For detailed information about this new curriculum,

log onto slrma.org for more information.