POLICIES, FOIA AND RECORDS RETENTION

Technology in your township

Like everyone else these days, townships rely on technology in a variety of ways. Townships keep, store and exchange more and more of their data electronically. Requests for township data are emailed or faxed to officials and employees. Data is requested in electronic form. We are often shocked when we learn someone does not have email.

This changing technological world also impacts a township's responsibilities when it gets dragged into court, and even as an employer. Courts demand that townships, and all other litigants, preserve electronic data for discovery and "production of documents" purposes. As to township employees, the state Legislature recently enacted a law limiting townships' and other employers' access to, and use of, personal social networking and email accounts of potential (and current!) employees.

Therefore, it is critically important for townships to consider and have in place specific policies and practices to address these ever-changing demands related to their electronic information and how to lawfully use technology to their advantage.

YOU MUST FOLLOW STATE RECORD RETENTION SCHEDULES

Public records of a township are also the property of the state and can only be disposed of or destroyed in compliance with Michigan law. To provide general authorization to dispose of public records, the state has adopted **record retention schedules** that provide the only legal authority to destroy public records. All townships must follow the General Record Retention Schedules for townships and local government services areas, including General Schedules No. 25, Clerks, No. 29, Treasurers, and No. 10, Township Records, which covers township records not covered by another schedule, as well as the general schedules for elections, law enforcement, libraries, fire/ambulance, human resources, information technology, financial records, and parks and recreation.

YOU NEED AN ELECTRONIC DATA RETENTION POLICY

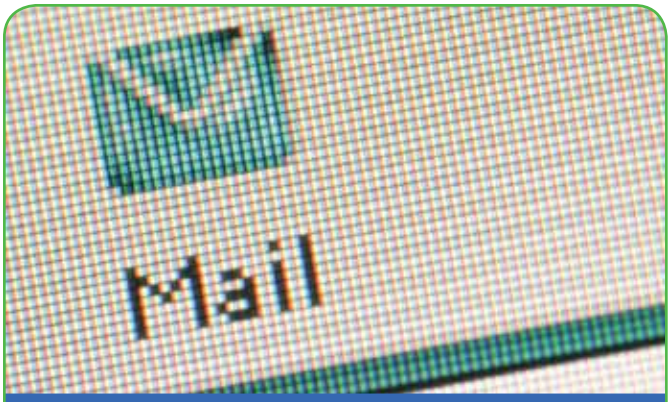
In addition to state retention **schedules**, internal document retention **policies** are required for legal, audit and practical reasons. Retention policies establish how long various types of information must be maintained in township files, and they should describe the procedures for retaining documents, guidelines for destroying documents, and special procedures for handling information when the township is involved in litigation.

The pervasive use of email, documents stored in electronic formats and the fact that we now seem to do everything "online" has greatly complicated dealing with an age-old issue. Most obvious, email has had a huge impact on the development, and enforcement, of record retention policies. That said, electronic data needs to be retained and managed like the paper copies of old for purposes of legal and management requirements.

In addition to changes in our behavior and our increasing comfort with computer systems, networks and the Internet, storing data has never been so easy or cheap. We now have massive amounts of data stored on huge, remote file servers so the limits of our desktop computers no longer apply. In this environment, we have a tendency to simply "save" everything that comes across our desks. And the increasing use of remote access means that township officials and employees may conduct township business from a location far from the township hall and the township's computers. Certainly, we all have many examples of the same information being stored by multiple people on multiple computers in various locations. There is little doubt that we all can point to the same Word document or Excel spreadsheet being stored in an official's laptop at home and in the township's server. And finally, there probably exists a hard copy from a meeting someone attended and another version stored off-site on a back-up tape!

THE FREEDOM OF INFORMATION ACT

The first, and most obvious, consideration that must be addressed in any township record retention policy is the Freedom of Information Act (FOIA), Public Act 442 of 1976, MCL 15.231, *et seq*. Every township should already have policies in place to address requests for documents under the FOIA. That policy should address electronic data as well. As MTA has explained in various educational sessions and resources on the topic:



Digital files and email messages are subject to the same laws and rules as "hard copy" (paper) records.

- Digital files and email messages are subject to the same laws and rules as "hard copy" (paper) records.
- Email, texts, Word documents, PDFs, etc. are no different from paper documents.
- You determine if it's a public record based on the individual files or messages—NOT the form it is in.

Employees who use a home computer and a personal email account to conduct township business must manage their work-related digital files and email the same way as those digital files and email messages that are created and received using township computer resources.

The FOIA limits the fees that townships can charge for public records, primarily to actual, incremental costs. However, the Enhanced Access to Public Records Act, Public Act 462 of 1996, MCL 15.441, *et seq*, allows townships to charge more than just actual, incremental costs to provide access to a geographical information system (GIS) output, or enhanced access to digital records. An example might be providing assessing or tax information on the township's website through a software module that the township purchases or subscribes to. A "reasonable fee" may be charged to allow the township to, over time, recover those operating expenses directly related to the provision of enhanced access to public records.

MTA's publication, An Introduction to the Freedom of Information Act*, offers an overview of FOIA, including requirements, handling requests and what constitutes of "public record." Cost is $22 for MTA-member township officials; $32 for non-members. Order online at www.michigantownships.org or call (517) 321-6467.*

THE LITIGATION 'HOLD'

The possibility of litigation also impacts township record retention policies and practices. Regardless of the specifics of your township's policy, when the township is threatened with or directly involved in litigation, special rules must apply. The law requires all data that *might* be related to the lawsuit ***or*** anything that is likely to lead to the discovery of admissible evidence *must be retained* and provided to the lawyers upon request. This rule is intended to prevent accidental and intentional destruction of potential evidence.

Electronic data needs to be retained and managed like the paper copies of old for purposes of legal and management requirements.

This becomes especially tricky in the case of electronic data. It is vital that the township be aware of practices or procedures that might inadvertently violate these rules. For example, if the township has programmed its email server to automatically delete email "trash" after one year and a day from the date of its creation, this kind of automatic deletion could violate the requirement that all evidence be preserved when there is a lawsuit pending against the township. If the litigation is a civil case, meaning cases like a claim for damages, a township could be accused of destroying potential evidence. If this occurs, a judge can allow a jury to draw an "adverse inference" if the judge determines that destruction of evidence has occurred. This means that the jury can infer whatever they like from the situation.

KEYS OF A DOCUMENT RETENTION POLICY

Townships are encouraged to periodically review their record retention policy to ensure that it addresses changes in document creation and retention. For example, if your policy was created before members of your board began using laptops, home computers, and smart phones, does it address those issues?

Ask yourself and others on your township board or in your administration these questions:

1. What is the purpose of your policy?
2. Who is covered by the policy? Are there certain requirements or limitations that apply only to a few departments? For example, how will your township address fire/police personnel posting pictures to social media of a scene or a crime?
3. What type of data and electronic systems are covered by the policy?
4. Are key terms, especially legal and technical terminology, defined?
5. Does the policy describe in detail what the retention, destruction and disclosure requirements are from both a legal and "business" perspective?
6. Does the policy clearly outline the procedures for ensuring data is properly retained, particularly with respect to electronic data such as email?
7. Does your procedure clearly outline the procedures for proper destruction of documents and information?
8. Does your policy clearly set forth what happens to document retention and destruction if there is litigation threatened against the township or if you receive discovery requests? Does it identify who is responsible for issuing a "litigation hold" memo, if one is required, and ensuring that your IT systems are managed consistent with the hold?
9. Does your policy identify who is responsible for data retention?
10. Does the policy explain the consequences for violating it?

The policy should be drafted not only with an optimistic mindset, but also a practical one. Understanding your township's particular practices and past history while brainstorming about the various ways data or documents could be destroyed, lost, damaged, altered or misused can lead to very strong—and realistic—retention policies.

EMPLOYMENT-RELATED CONSIDERATIONS

Through the course of their employment, township employees gain access to information about and data belonging to your township, its citizens and other employees. We would be remiss to present technology considerations without emphasizing how inter-related data retention and disclosure policies are with employment matters. Here are just a few of the common concerns:

Confidentiality. A document retention policy, like any other policy, is only as effective as its enforcement. Confidentiality policies can greatly assist townships in managing and securing their data in this digital age. Township employees can—and should—be required to acknowledge the township's confidentiality policies.

Acceptable use policies. Townships should establish an acceptable use policy for its technology systems in order to encourage proper and lawful use of township property and systems. Although townships can define technology systems as broadly or narrowly as they like, this term typically includes telephones, facsimile machines, photocopiers, computers, printers, voice mail, email systems, and other technology. Acceptable use policies should address use of personal communication devices during the work day, use of recording devices, such as cameras, camera phones and tape recorders. These policies should also address sending, receiving or accessing pornographic, discriminatory, harassing, or otherwise unlawful materials or purposes. Other items that may be addressed: causing congestion, disruption, disablement, alteration or impairment of township networks or systems, maintaining, organizing or participating in non-work related blogs, websites, journals, chat rooms or instant messaging, and failing to log off secure, controlled-access computers or other

forms of electronic data systems, playing games, or attempting to hack into or avoid security restrictions on township systems and applications.

Make sure the acceptable use policies also clearly explain that violation of the policy may result in disciplinary action, up to and including discharge.

Solicitation policies. Office email has quickly become the bulletin board of the digital age. But even the most generous souls will tire of constant email solicitation from their co-workers about laudable causes, events or upcoming legislation. We encourage townships to consider how their solicitation policies apply to office email, especially emails exchanged during working time.

No expectation of privacy on township systems. Townships should also carefully advise employees that it has the right to and may monitor, review or access electronic data stored on its technology systems. Notifying employees that they have no reasonable expectation of privacy in any communication or information conveyed or stored on township systems is critical. This also provides some protection to townships when managing discriminatory, harassing, illegal, immoral or other questionable conduct by employees that might occur through use of information or communication sent or stored in its technology systems.

Personal use of township equipment, supplies and property. Management and protection of electronic data and hard copies of vital township documents also requires management of employees' personal use of township equipment, supplies and property. Townships should set clear expectations that personal use is unacceptable to further solidify the message that protection of township information, data and documentation is critical. Thus, township policies prohibiting personal use of township property, equipment, machines, supplies, postage, and the like, except with prior approval or authority, can help townships protect their information.

Employees represent the township. Employers, including townships, have long struggled with how to manage circumstances where employees represent themselves as speaking for the township or as having some special knowledge or authority. The technology advances we've described here have only further complicated this matter. Emails can be shared at the click of the mouse to hundreds of people, often without the original sender's knowledge, let alone permission. Employees can create personal social media accounts, log onto chatrooms or instant messaging, create blogs or video blogs and speak "from the township perspective" when no such authority was granted.

Townships should carefully address these issues in employee handbooks, keeping in mind that there are limits to the restrictions employers can place on employee speech.

Contrast this with the circumstance where a certain township employee or official is responsible for updating a township website, or maintaining and improving a township social media account. There, the township can—and should—exercise greater control over what goes on and in these sites or accounts. ▶

New law impacting townships' access to employees' personal email and Internet accounts. Without question, the Internet and its instant availability of information about potential and current employees has changed the landscape of employment screening and management. Concerns over cyber security and protection of private Internet accounts in employment settings led to the state's Internet Privacy Protection Act, which was signed into law in the last few days of 2012.

The act generally prohibits employers (including townships) from requiring employees or applicants to provide access to or information from the individual's personal social networking accounts. Townships, therefore, cannot demand that an employee or prospective employee provide their passwords or login information, or show the township his or her private Internet account or social media site, whether it's Facebook®, Twitter®, LinkedIn®, or something else.

There are a number of exemptions, however. For example, townships may still demand access to township-owned or paid electronic communications devices, and access to email and social media accounts when accessed on or via a township account or service. Townships may also compel employees to cooperate in investigations in certain cases.

This law does not require townships or any other employer to search or monitor its employees' personal Internet accounts. This is, of course, important for a variety of situations, including limiting or eliminating the townships liability to become aware of workplace violence or harassment that may be perpetrated primarily through social media or personal email accounts.

The increasing use of remote access means that township officials and employees may conduct township business from a location far from the township hall and the township's computers.

The law, importantly, does not prohibit or restrict townships "from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain." Thus, townships can still browse Facebook® and other social media or Internet sites to gather potentially valuable information about an applicant or current employee—they just can't demand that the employee or applicant give the township access or information from those social networking accounts. If an issue arises in your township involving employee social media or private Internet accounts, consult with your township attorney to determine the extent to which this law could impact your township.

Grounds for discipline or discharge. Many townships work primarily with independent contractors or employ individuals in an at-will capacity. Others have collective bargaining agreements with one or more bargaining units, be it clerical staff, police or fire departments. In any case, it is critical to establish an expectation that the following are prohibited and could result in discipline, up to and including discharge:

- Unauthorized use of township property, equipment or facilities.
- Unauthorized use of township telephones or other technology systems for personal use during working hours, or use or possession of another employee's personal equipment or possessions without the employee's consent. (Note that certain organizing actions under labor laws may be protected and not "personal" use.)
- Unauthorized removal of any property or records from the township.
- Falsifying or omitting pertinent information from records or revealing confidential information to unauthorized persons.

Doing so supports prompt action by the township where necessary to protect, repair or retrieve township data or address an employee relations issue involving township data, technology systems, and the like. This type of support, be it in rules of conduct, employee handbooks or contracts, can be critical in resolving what might otherwise become a sticky, tricky situation.

Townships may wish to and should consider taking advantage of this technological age in which we live. For example, keep regularly reviewed and updated documents in an accessible word-processing format for easier edits. Think about the next time the township will have its township attorney review and update the township employee handbook. If the handbook is in a word-processing document already, those revisions can be accomplished much more quickly—and more cost-effectively—than if the document must be typed from scratch.

Accessibility in the technological world. Although there are certainly those township employees and officials who do not have cell phones or email addresses, there are many, many who do. And often these cell phones, iPads and other portable electronic devices enable the township employee to perform township work when outside of the township hall, before or after the normal workday. Townships should recall that there are possible wage and hour issues with encouraging—or turning a blind eye to—such hyper-connectivity. State and federal wage and hour laws require employers to pay employees for time worked and in some cases, the state and federal agencies responsible for investigating and enforcing wage and hour laws have been focusing on the frequency and tracking of employee off-site access and work on behalf of an employer. (Note that township board members are not employees for this purpose.)

TACKLING THE TECH

Whether your township has embraced technology's role in local government administration or is fending off the digital age, there are many considerations that come into the mix. As with everything, there are benefits and drawbacks to these advancements, but the key is that townships understand the variety of ways technology can—and will impact—them and their employees and residents, and address them now. ■

Steve Schultz,
President and Attorney,
and **Helen E.R. Mills**, Attorney,
Fahey Schultz Burzych Rhodes PLC,
Okemos

Contact Schultz and Mills at (517) 381-0100, or via email at sschultz@fsbrlaw.com or hmills@fsbrlaw.com. You can also visit www.fsbrlaw.com for more information.