

Personal Digital Devices

Given the prevalence of portable digital devices, it is no surprise that many employees are using their own personal devices to perform state work. This practice is often referred to as Bring Your Own Device or BYOD. BYOD raises many issues and concerns for records management practices and is not the easy, cost effective solution that some agencies may consider it to be.

Data Management

A BYOD policy makes it difficult-to-impossible to ensure that proper information practices are being followed by the operator of the device. If an agency finds itself in a lawsuit, an auditor will want to know what steps the agency took to ensure that the data in question was adequately protected on an employee's personal device.

Security

There is always concern about security when it comes to personal devices.

- **Lost or Stolen Devices** – One potential security issue that arises with the use of BYOD is the potential for employees to lose their personal devices containing unsecured data. Depending on the scope of work of the employee or the agency involved, sensitive information may land in the wrong hands.
- **Malware** – There is always the potential for an application downloaded to a portable device to contain malicious software that may compromise the device in use and any information contained on it.
- **Disgruntled employees** – Unfortunately, not all employees leave an agency on good terms and, if disgruntled employees have sensitive information on their personal devices, they may choose to publish or disseminate information not meant for the public.

Privacy

One concern an employee should have with a BYOD plan is the potential for a breach in their privacy. If information on a personal device is needed for legal reasons, a search of the device will not only yield the state records but also any personal records such as email that may be on the device. All the information on the device would have to be preserved for discovery purposes and a "wipe" or complete erasure of data would not be possible because of the legal obligations involved with state records.

An agency with a BYOD policy may open itself to the possibility for a multitude of legal and privacy issues. If a portable device or laptop computer is needed for an employee to complete essential job duties, best practice would be to issue a state owned device that has the proper IT support to accommodate security and discovery issues.

Social Media

Social media is a broad term that incorporates various web based technologies such as blogging, video sharing, wikis, social networks, and photo libraries. Most state agencies operate one or more social media accounts which has added another dimension to records management. *Social Media Records*

Social media provides another avenue for agencies to engage with the public and to collaborate internally. One of the challenges presented by social media is the identification of a record. An entry on a social media site might not always constitute a record. The following should be considered when trying to determine if an entry on a social media site is a record:

- Does the social media content contain information or evidence concerning an agency's mission or policies?
- Is the information unique or available elsewhere?
- Does the social media content contain evidence of official agency business?
- Does it document a controversial issue?
- Does it document a program or project that involves prominent people, places or an event?

If the answer to one or more of the above questions is yes, then the social media entry is a record.

Unless the content created in social media denotes a new record series, social media records will most likely fit in the characterization of an existing record series such as press releases. If the social media records indeed represent a new records series, the RRS should be updated to reflect the new series. URLs for sites or for feeds can be included in the remarks column of the RRS. The State Archives will then have the opportunity to flag any appropriate social media for archival retention. If social media records are flagged for archival retention, the State Archives may subscribe to the feeds and/or request that the state agency preserve and then transfer files at the end of the retention period. If social media records are not flagged for transfer to the State Archives, the agency must then destroy social media records upon the end of their retention period.

If, in fact, a social media entry is considered a record, it must adhere to a record retention schedule policy and practices. The issue of how to capture the record arises. Social media records can be more complex than traditional electronic records given their ability to allow enhancement with additional comments, metadata, or other information. A plan to export records from a social media site to a recordkeeping system is important and should be created in collaboration with an agency's IT department. There are web crawling tools and software to capture social media entries but these may prove cost prohibitive for an agency. Storing the original content, such as a video, elsewhere beyond the social media site may suffice for ensuring retention of a record. An agency could also keep a file of blogs and social media entries, which would at least ensure that the original content would be retained.