Aardsma Archives *prepare well. protect well.*

Include Copiers in Data Security Plans

IT CAN BE A VULNERABLE PART OF YOUR NETWORK

Currently, it seems everything has a built-in hard drive—cell phones, cable TV boxes, and even cars. Church leaders may not realize that most newer copy machines feature onboard hard drives that can store images of every document the machine prints. This can present a data security threat, but there's plenty you can do to protect your ministry's sensitive information.

Copier hard drives can make some tasks more convenient. Instead of searching for an often-used document on a computer or in a file folder, documents can be recalled from the copier's memory for quick printing. However, without proper security measures in place, a copier may save every document it prints to its hard drive, possibly making sensitive information available to anyone with access to the machine.

Most copier manufacturers offer data security features, although some cost extra to install. These features include:

- **Encryption.** When encryption is activated, the information is scrambled before it is stored in the machine's memory. Encrypted data can be read only by certain software programs, even if the hard drive is removed.
- **Overwriting.** Some machines offer overwriting as a scheduled cleanup task. The U.S. Bureau of Consumer Protection recommends overwriting the entire hard drive at least once a month, but the more frequently this is done, the less likely that information could be compromised. Some machines allow users to overwrite after each print job.
- **Passcode locks.** The hard drive contents can be passcode-protected. Without the code, users cannot access saved documents.

(Continued page 2)

Churches may connect their copier to a computer network and use it as their office printer (and, in some cases, their scanner and fax machine). As a result, it may be possible to access the copier's hard drive from remote locations. Consider the network's security situation and how the copier is protected from these risks. If the church doesn't have a qualified IT person, it may be a good idea to consult a qualified vendor to handle security issues like these.

When the ministry copier is returned at the end of its lease, traded in for a newer model, or sold, the manufacturer, dealer, or service provider may provide options for securing any data left on the hard drive. These options often include removing the hard drive and returning it to you, or overwriting the files for you. It's wise to understand—in advance—which options are available, and which solution your ministry will use.

Protecting the data on a copier's hard drive is often as simple as understanding the machine's security settings and using them appropriately. By taking steps to protect these hard drives, ministries can better secure their own sensitive information—and that of their members.