BYOD (Bring Your Own Device)

Implementing a BYOD program within a non-profit society is a great way to reduce costs associated with employee mobility while at the same time increase employee productivity and reduce the need of an employee to manage multiple devices. But there are risks associated with a BYOD policy which a society's management and board should be aware of, including:

1. Opportunities for Data Theft – Employee improperly handling sensitive society data and personal information of clients. This is very prevalent with email.
2. Malware Infiltration – Not having proper protection on a device could allow for data theft from outside sources or allowing the malware onto your society data systems.
3. Potential Legal and Reputational Issues – A society's reputation could be jeopardized if information is leaked or stolen from the device.
4. Device Loss or Theft – Data on the device could be vulnerable if there is inadequate password management improving the chances of hackers accessing sensitive and personal information.
5. Poor Mobile Management – If an employee leaves your organization for any reason, they may be walking out the door with sensitive and personal data, or may also continue to have access this data.
6. Lack of Training – If employees are not fully trained on how to protect the data on the devices, mistakes can be made, and data could be exposed.
7. Public WiFi – Connecting to Public WiFi, depending on the terms and conditions being agreed to, could allow capturing of information with no determination of what is personal and sensitive. If something is free to you, always think about what is in it for the other party? And not all public WiFi hotspots provide an expected level of security to protect the user.
8. Employee Termination – If there are no controls over the device, personal and sensitive information could remain after the individual leaves the organization.

It's important to recognize that there is a legal requirement within PIPA to maintain control of personal information collected by a non-profit organization. By accessing work information on a personal device, an employee puts a non-profit's assets and reputation at risk

To manage BYOD risks, non-profit organizations should implement defense strategies; unsurprisingly, many defenses can reduce employee privacy. For example, non-profit IT department administrators may install remote access apps on personal devices, so administrators can access information and control the device when necessary. If an employee's phone becomes compromised, the administrator can access the phone remotely and delete any sensitive organizational data.

Unfortunately, when such a remote access app is installed, personal documents like photos and videos may be accessed and deleted as well. The administrator may also be required to safeguard information by blocking network access, apps, and websites

on personal devices. Non-profit employees may view these acts as breaches of privacy or personal rights.

Aside from data breaches, top BYOD concerns arise from the employment relationship.

- Workplace safety risks: While driving, employees may talk on personal devices that are used for personal *and* work reasons.
- Labor law risks: IT safeguards protecting a non-profit's reputation and assets may be considered unlawful surveillance of employees.
- Wage and hour risks: Personal work devices used off-the-clock for business purposes may put the non-profit employer at risk of liability for overtime time pay.
- International risks: When employees travel abroad, border guards may access sensitive data while searching devices.

BYOD use also exposes non-profit employers to the potential for leaked sensitive and/or personal information, and the risk of employees uploading materials to servers owned by other companies (e.g., through the use of cloud apps like Dropbox or Google Drive). It is recommended to put the following safeguards in place:

1. Create a clear policy on BYOD rights and information security rules.
2. Train employees to protect work information accessed on personal devices.
3. Require employees to sign an agreement acknowledging their role in protecting confidential or personal information stored on or accessed by personal devices.
4. Require employees to sign an agreement acknowledging the actions and steps an in-house or outsourced IT team may take to protect information stored on or accessed by personal devices.
5. Establish a protocol for wiping work-related information from lost employee devices or when separation from employment occurs.
6. Ban employees from moving funds into or out of non-profit bank accounts using personal devices.
7. Prohibit non-exempt employees from accessing work email or making work-related calls outside of work hours or establish clear guidelines with appropriate accountability measures permitting work outside approved schedules.
8. Implement Mobile Device Management software on the device to improve control and visibility of organizational personal and sensitive information.

No matter how many BYOD policies you create, risk remains. An society's IT department charged with securing non-profit data can offer only partial protection for data stored on devices the non-profit doesn't own. But, even if you stick to organization-owned devices, data breaches may occur. Weigh the upsides and downsides of BYOD before making a decision.