GRAND VALLEY PUBLIC LIBRARY BOARD
POLICY MANUAL
Human Resources, Social Media

Date of Approval: December 11, 2013   Motion #:   7

Chairpersons Signature:

Policy Title: Computer, e-mail, personal e-devices, personal phones and Internet Use

Chairperson's signature: _____

The Grand Valley Public Library Board recognizes the importance of computers, the internet and social media as work tools and sources of information. The library supports the use of computers and internet technology by staff in their work while recognizing the need to protect its network, systems, resources and the library's image.

Section 1: Personal Use

1. While working in the library, staff must refrain from online activities, e-devices and phone calls that don't bring value to the library. Staff may make reasonable personal use of computer equipment, access to the internet and e-mail provided by the library on their own time, provided it does not adversely affect their work or the work of others and has minimal effect on the library's resources.

2. Computer resources cannot be used for private financial gain or commercial purposes.

3. When engaging in social media outside of work, staff should make it clear that the views they express about the library, or community related issues, are their own and do not necessarily reflect the library's view.

4. Personal use of social media should be respectful of the library, colleagues and library clients. While online activity can be a medium of self- expression, it may be very public and reflect on both the individual and the library. Social media means any tool for online publication and commentary, including blogs, social networking sites such as Facebook, and You Tube.

5. Downloading software or attachments onto a work computer increases the risk of a virus infection throughout the network. Staff should consult with their supervisor before downloading files or software.

Section 2: Business Use

1. Staff is encouraged to avail themselves of the internet, including social media tools for the benefit the library. This may include general research on work related issues, following social media as part of ongoing professional development, staff or user training, and participating in on-line communities.

2. Any correspondence sent from a library's email address should be treated as a professional document even if it just a one-line reply.

3. Staff should consult with their supervisor before posting comments to blogs or social network sites as an employee of the library.

4. When posting to any social media site as an employee, communications must be professional and posted information must be accurate.

5. Staff must observe the library's standard of confidentiality (e.g. privacy legislation) when communicating electronically.

6. Downloading software or attachments onto a work computer increases the risk of a virus infection throughout the network. Staff should consult with their supervisor before downloading files or software.

7. All staff have an obligation to protect systems and data. Passwords and access codes must not be disclosed to unauthorized staff or the public.

Section 4: Prohibited Use:

1. The library's computers, network and access to the internet are not to be used to:

   a) undertake deliberate activities that waste staff time or networked resources.
   b) introduce any form of malicious software into the network.
   c) visit internet sites that contain obscene, hateful, pornographic or illegal material.
   d) perpetrate any form of fraud; software, film or music piracy.
   e) hack into unauthorized areas
   f) send offensive or harassing material to other users

Section 5: The Library's Social Media Presence

1. Any proposal by staff to use social media applications to expand library service or promote the library requires the approval of the CEO

2. Staff representing the library on social media sites express the official position of the library on any issue.

Section 6: Misuse

1. Staff will be accountable to their supervisor and the CEO for their use of the library's computer network and internet access.

2. The CEO, or her designate, will investigate any suspected misuse of resources.

3. If there is a need to monitor or access non-work related files, the staff member will normally be asked for his/her consent. There may be exceptions such as when there is reason to believe the law has been broken.

4. The CEO will decide, in light of the outcome of an investigation of possible misuse of computing resources, if disciplinary action is appropriate and act in accordance with established disciplinary procedures.