PINEBROOK BIBLE CONFERENCE COMPUTER / NETWORK / SOFTWARE POLICY (Revised date 12/01/12)

The purpose of this policy is to outline appropriate use of company computers, software, e-mail, and internet.
These procedures are necessary to protect our hardware and software investment, maintain network integrity and
preserve available bandwidth for business applications, maintain the security of our confidential data, and focus on
human resources on our mission and ministry.

- Company owned computers shall not contain software of any kind which is not owned by and licensed to Pinebrook Bible Conference unless requested in writing and approved in writing by the Director. Employees may not install downloaded or personal sofware on company owned computers. This includes, but is not limited to, instant messaging programs, desktop themes, screen saver programs, browser plug-ins or toolbars, games, audio and video players, erase and purge utilities, etc. An exception to the above is that non-offensive personal pictures may be used as Windows wallpaper or slide-show screen saver.

- Company-owned computers and software, with the exception of those computers designated as Staff Benefits computers, may not be used in any way for purposes not directly related to work performed for the company. Prohibited activity includes, but is not limited to, playing games, surfing the Internet, creating personal letters or greeting cards, viewing or editing pictures, personal banking, online shopping, streaming applications including internet radio and video. Staff Benefits computers may be used for personal business and internet access provided it is not on paid company time. Internet access must still comply with all other aspects of this policy.

- Employee use of the internet and e-mail may be monitored and/or audited for misuse. Content Filtering technology may be used to prevent the access of offensive web content. Even with content filtering, accessing any kind of pornographic, racist, sexist, threatening or otherwise objectionable subject matter is expressly prohibited. Requests to unblock sites where access is needed should be made to the Pinebrook Director.

- Employees with access to the internet and/or e-mail are restricted to its use for specific and defined job purposes only.

- Employees who want to use their own computer on a Pinebrook network for internet access must first contact the Director to establish that the computer meets minimum requirements for security and anti-virus. Once this is done, and if the office has network wiring which will allow the connection it will be set up by the IT Supervisor.

- E-mail will be assigned to every permanent employee. Employees are required to check their Pinebrook e-mail at least once per day to ensure they are apprised of procedures updates, schedule changes for meeting etc. Employees may choose to forward their Pinebrook e-mail address to their personal e-mail. However, be aware that because our e-mail guidelines encourage users to ignore and delete potential spam, replies sent from a personal e-mail might not be recognized or opened by Pinebrook employees if the address is unfamiliar.

- Company e-mail is company property. Hourly and salaried employees may not send or review personal e-mails during paid working hours. Under no conditions may company e-mail be used for solicitation. All company e-mail is accessible for monitoring or good cause audit by Pinebrook information technology staff. “Good cause” shall include the need to protect system security, fulfill company obligations, detect employee wrongdoing, comply with legal process, or protect the rights or property of the company. In the event there is a personal e-mail use while on company time, an employee’s e-mail address may be forwarded to a manager to assist an employee in policy compliance, and/or progressive discipline may be implemented.

- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages is prohibited.

- Installing instant messaging programs such as AIM, AOL Instant Messenger, Yahoo Messenger, Microsoft MSN Messenger, ICQ, etc., is prohibited. Facebook, Twitter, etc. must be deemed as Business justified to be used on a company PC.

- Computer login accounts, usernames and passwords may not be changed without the approval of the IT Manager. The logged-on user is responsible for activity on the computer, so passwords may not be shared.

- Computers with internet access will be set up to retain 90 days of internet browser history. This setting may not be changed, nor may the history, cache or cookies be purged without notifying the IT Manager.

- Causing congestion, disruption, disablement, alteration, or impairment of company computers or network systems is prohibited. Computer problems are to be reported to the IT Manager immedtiately.

- Introducing computer viruses, spyware, adware, or other disruptive or destructive programs onto company computers or networks is prohibited. Knowledge or suspicion of the presence of a virus, spyware, adware or any other system problem must be to the IT Manager immediately.

- Computers must be left on at all times to allow backups, Windows security and anti-virus updates to run at pre-scheduled times. Turning off computers threatens the integrity of the system safeguards and is prohibited.

- All documents and e-mails created using company computers, software or e-mail resources or residing on company computers are the property of Pinebrook Bible Conference.

- Wireless networks are particularly vulnerable to security breaches. Pinebrook laptop computers with built-in wireless (WiFi) capability may NOT be used to connect to any unprotected public or private wireless network.

PROCEDURE:

- All company software and equipment will be purchased by the IT Manager and held in a software library in a centralized administrative location. All software and computer-related hardware requests must go to the IT Manager.

- All internet access accounts, e-mail accounts, computer login accounts, usernames and passwords will be set up and maintained by the IT Manager. Login accounts, usernames and passwords may not be changed without first contacting the IT Manager.

- Computer security and confidentiality must be maintained to the fullest extent.

VIOLATIONS

- According to U.S. Copyright Law, illegal reproduction of computer software can be subject to civil damages of $50,000 or more and criminal penalties including fines and imprisonment. Pinebrook complies with software licensing requirements and will not tolerate behavior that violates law through the use of illegal software.

- The presence of child pornography (under18 year of age) on a Pinebrook computer will result in that computer being turned over to police for investigation, and the possibility of criminal charges.

- Violation of this computer software policy will result in disciplinary action which may include prosecution and discharge.

Date Read : _____ Signature : _____