

FILTERING/REPORTING SOFTWARE CHECKLIST

This is a recommended list of features to consider when selecting software applications intended to block, monitor, and/or report electronic activity on computers, mobile phones, iPods, etc.

- Resistance to Hacking
 - “Thin client”
 - Routes all electronic activity to a “cloud” of servers
 - Does not use your computer’s resources to store or filter data
 - Anti-tamper
 - Can shut down all internet access if any of the application’s files are manually deleted or altered
 - Requires a password for uninstall
 - No password override (option)
- Ability to block ...
 - Objectionable sites
 - Administrator can list specific sites to allow/deny
 - Administrator can specify different categories to allow/deny
 - Certain keywords for search engines
 - Banner ads and pop-ups
 - Peer-to-peer (P2P) software
 - Which applications on your computer are allowed to send data to the internet
 - Chats, IM, social networks, email (including disabling links & attachments)
- Recording of Activity
 - History of all websites visited
 - Chats and social network site activity
 - Capture screen/text when key words typed (e.g., bad words, personal info)
- Reporting (email, text, call, store files on computer or server)
 - Including instant alerts
- Time limits
- Miscellaneous
 - Can set up different settings for different user accounts
 - Scalable (load on multiple computers or apply to wireless/ethernet router)