BASIC GUIDELINES FOR THE PROTECTION OF OUR CHILDREN

PROTECT YOUR HOME

1. IF PARENTS choose to have Internet access in their home, a filter must be installed on each computer that a child can access. The filter must, at the very least, filter out adult content, violence, chat rooms, and social networking. The search must also be forced to "safe search". Any video sharing websites particularly "YouTube" are rife with extremely inappropriate video content and must be blocked by your filter as well. Optimally, a "white list" filter should be used which only allows pre-approved sites and blacklists all others. We have provided a list of effective filters (see the other side of this brochure). Should a parent, for any reason, require unfiltered internet access, the computer must be password protected, kept under lock and key, and never be accessed by children.

2. IT IS well documented that even the best of filters cannot be completely relied upon; even "safe searches" can bring up highly inappropriate material and images. Consequently, a child may never go online alone without a parent **and** not without a specified constructive purpose (e.g. project research).

3. EVEN IF the Internet access is filtered or disabled, computer use should always be monitored by parents. Computers should be located in open, family spaces and should never be in a child's bedroom.

4. IF PARENTS choose to have a WiFi network in their home, it must be securely password protected. If others in your vicinity have an unsecured WiFi signal, you should not hesitate to request that they secure it.

5. BEFORE ALLOWING a child to visit or babysit in someone else's home, parents should not hesitate to inquire what technology and/or digital media is available in that home. Based on the information received, they can make an informed decision whether or not to allow their child to spend time in that home. Likewise, parents who hire babysitters must be sensitive to those children's family values and standards, by not leaving any computers, laptops, DVD's, DVD players, etc, open or accessible.

6. IF PARENTS, for safety concerns, feel the need to provide their child with a cell phone, the data plan (Internet) must be turned off through the service provider. Cell phones should never be exclusive to a specific child but rather "family owned" and only given to a child on an as-needed basis.

7. UNDER NO CIRCUMSTANCES should a child have a personal email account or an account with Facebook, Twitter or any other social networking site.

PROTECT YOUR CHILD

It is important to note that although the WiFi access in one's own home will be securely password protected, in today's day and age, it is virtually impossible to create and maintain an environment that is completely WiFi free. Accessibility can come from many other sources, such as a neighbor or a mobile WiFi card that parents may be completely unaware of. As such, adherence to the following is of absolute necessity.

IF PARENTS DECIDE to allow their

8. children to use digital gaming devices, they should make sure that the devices cannot access the Internet. Unfortunately, all major gaming devices presently on the market, such as the Nintendo Wii, Sony Play Station, and Microsoft Xbox, have WiFi connectivity and, therefore, must be inaccessible to children. Parents must also familiarize themselves with the capabilities of all digital devices and the content of all computer games, no matter how innocent they appear or how low their ratings. Just because a game contains an "E" (everyone) rating does not mean that it upholds the values of one's individual home or society.

9. CHILDREN MAY NOT own or have access to any personal gaming or entertainment devices that have WiFi connectivity, e.g. iPod Touch, Sony PSP, Nintendo 3DS, Sony PS Vita, and Nintendo DS-I. Access to these devices is tantamount to open and unfiltered access to the Internet.

10. CHILDREN CAN NEVER be given their own laptops, notebooks, DVD players, or iPads. These devices can all too easily afford them unsupervised and unfiltered access to the Internet and other inappropriate videos or digital media.

11. IF PARENTS DECIDE to purchase a non-video iPod or MP3 player for their child, its usage and content must be monitored regularly. Optimally, parents should be the ones to load the content. If children have access to memory cards or USB storage devices, also known as memory sticks or flash drives, their content must likewise be closely monitored.

The above guidelines are the basic minimum השתדלות incumbent upon us as parents in the safeguarding of our children in today's society. בזכות our adherence, may the רבונו של עולם help us raise בנים ובנות צדיקים וצדקניות. אמן

T.A.G. INFORMATION & HELP LINE

732-730-1824 (1-TAG)

INTERNET FILTER & MONITORING OPTIONS

FILTERING

Filtering attempts to block unwanted content. *This can be accomplished in 3 ways:*

1. By creating a whitelist with companies like NativUSA where only websites specifically deemed as appropriate can be accessed.

2. Utilizing a blacklist where the entire web is open and the filter attempts to block problematic content by categorizing each website *(e.g. shopping, travel, adult, etc.)*. This is the most common approach and many use the K9 filter for this.

3. The most innovative approach to filtering being pursued by companies like Venishmartem Cloud Filter is dynamic filtering where each website is evaluated for content in real time as it is loading.

MONITORING

Monitoring, provided by programs such as Covenant Eyes and Spector Pro, allows free access to all websites and content but provides a report to a designated monitor about web activity.

Knowing that one is being watched may serve as a deterrent from accessing inappropriate content and if a person has a problem it may be addressed. It is also important for parents to be aware of their children's' digital habits so they can guide them in this area. However, monitoring alone affords no protection from accidental accessing of websites.

In summary, filtering is the minimal form of necessary protection for any computer and monitoring is recommended as an additional level of protection and oversight.

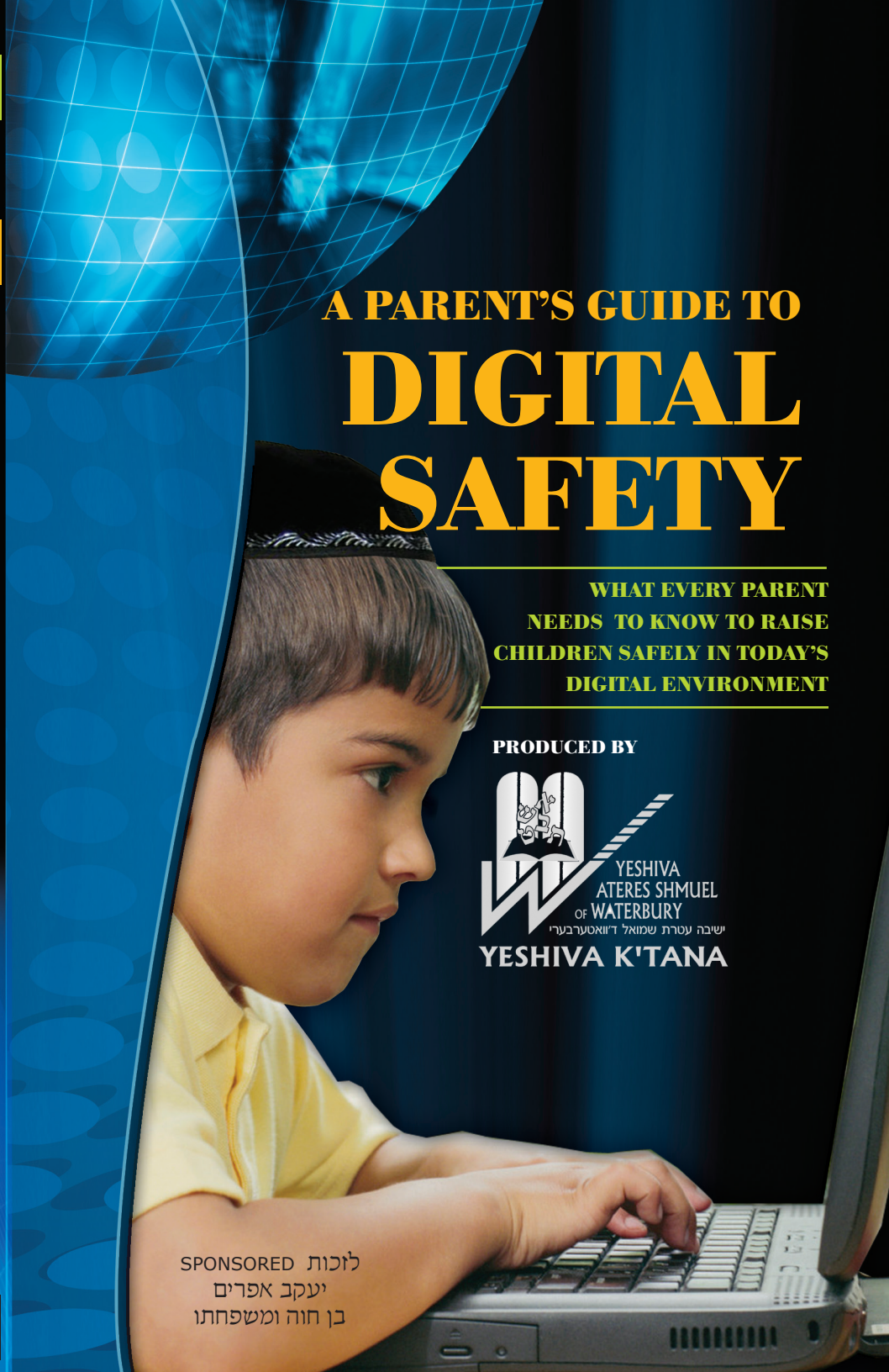
In practice choosing the appropriate filtering/monitoring software package for your family is complicated. There are many variables to consider in creating the optimal balance between the freedom to pursue the necessary and the imperative to shield from the harmful. With this in mind we urge you to take advantage of the services of TAG and seek their expert advice and guidance on the best filtering/monitoring package to suit your needs.

REMEMBER THERE ARE METHODS TO CIRCUMVENT EVERY FILTER
The most prudent step is to remove all Internet access from your home!

FIVE STAR DESIGN 732.905.5842

A PARENT'S GUIDE TO DIGITAL SAFETY

WHAT EVERY PARENT NEEDS TO KNOW TO RAISE CHILDREN SAFELY IN TODAY'S DIGITAL ENVIRONMENT



PRODUCED BY

YESHIVA ATERES SHMUEL OF WATERBURY
ישיבה עטרת שמואל ד'וואטערבערי
YESHIVA K'TANA

SPONSORED לזכות
יעקב אפרים
בן חוה ומשפחתו