CHAPTER ONE

Safety and the iPhone: Managing restrictions

Managing risks

There are risks with using a smartphone. Risks of compulsive screen use that interferes with work, school, exercise and social development. Risks of online crooks stealing money by password theft and scams. Risks of predators taking advantage of a vulnerable population.

These are all real risks, but there are bigger risks out there. In the city where I live a pedestrian is killed by a motor vehicle every other day — and we aren't a particularly big city. My Explorers run real risks when they travel to work or school. The connectivity and on-hand support of a smartphone can reduce the big risks Explorers face even as they bring smaller risks of their own.

That doesn't mean we should ignore smartphone risks. There are practical things Guides can do, such as using phone "restrictions", protecting Explorer passwords, doing regular remote monitoring, making sure smartphones are being backed up (see Backups), and regularly showing Explorers examples of scams we all see daily. In this chapter I'll review what works. First though, I'll address something that doesn't work.

Watching what your Explorer does - good luck with that.

We've all heard advice that parents need to be aware of what their kids do online. Advice that is almost never followed by any practical explanation of how to do that. That advice drives me a bit crazy. Have any of these people ever tried to stand over a teenager and watch what they do online? Do they even have a life?

Even when all we had to worry about was large screen computers, perhaps used in an easily monitored family area, this didn't work very well. Teenagers are fast, and they have great hearing. With personal smartphones this poor advice is even less useful.

I'm not going to advise Guides to "watch" what their Explorer's do. Instead I'll

review practical measures using restriction abilities built into iPhones and available for Android, starting with how restrictions line up with individual Explorers.

Growing towards independent use

Explorers are a diverse group, just like neurotypical teens and adults. The main difference between Explorers and neurotypical adults is that many Explorers have legal guardians, and most have an extended period of formal guidance. During this period of extended support Explorers may go through the usual progression that neurotypical youth experience — from restricted or monitored computer and media use towards unrestricted use. Most won't have a smooth progression though — they will run into issues along the way. Many Explorers will be vulnerable to exploitation — often financial but also personal. Others may be prone to screen abuse; neglecting personal growth and development for the games and online activities. Sometimes Explorers will take two steps forward and one step backwards.

It's useful to consider a set of five steps, from a very safe level appropriate for all ages and temperaments to Guide-free use. The first step is safe for all users, later steps require better Explorer judgment and/or more monitoring.

Step	**Description - particularly restrictions**
1	Calendar, Notes, Contacts, Weather, Maps, Find Friends. Media content age restricted. Introduce apps incrementally. All installations by Guide including selected maturity-appropriate games and media. Explorer cannot install or delete apps. Explorer does not know any passwords except smartphone unlock code (or use fingerprint unlock). No online access, no messaging or email.
2	Add web access limited to specified sites. Explorer may manage own music library or subscribe to a Cloud service.
3	Add messaging and email. Guide routinely monitoring. Explorer can browse App and media stores but purchase requires Guide. Age limits may apply to Apps and media.
4	Add Facebook. Consider automated filtering of web sites rather than specified list. Explorer may be able to purchase and install apps. Guide continues to monitor. Explorer may know some passwords but not change them.

5	Unrestricted, including purchasing and YouTube. Full app installation and deletion privileges. Guide does not monitor or monitors intermittently. Explorer may know all passwords and may change them.

Most Explorers will start at Step 1 or 2. At these levels many restrictions will be in place and a Guide is teaching and coaching and adding or removing apps and media. Explorers will usually progress over time to Step 3 or 4. These levels usually require regular remote monitoring by a Guide.

Step 5 is where most independent living adults are. Some Explorers may take a while to get there, some never will. As always Guides will need to adjust expectations and restrictions to an individual Explorer.

I'll go over typical issues and how they change an Explorer's level, including screen abuse problems. First though I'll talk about how to practically assign an Explorer to one of the above five Steps.

Restrictions and parental controls

As a Guide you've done basic setup of an Explorer's smartphone. You've also evaluated your Explorer and decided they should be using their smartphone at Step 1. Great! Now what do you do?

The good news is that there are ways to configure both iPhone and Android phones to limit what they can do. These "restrictions" or "parental controls" weren't created to help Guides, they were created for parents, schools, and corporations to use. Happily they can work for Guides and Explorers too. (Though it would be great if, in future, Apple and Google were to consider the *unique* needs of Explorers.)

Restrictions allow a Guide to control software installation and deletion, to prevent changes to account settings, and to restrict media and internet access.

How a Guide uses these restrictions to match a smartphone's abilities to an Explorer's needs is quite different for iPhones and Android phones. Apple's iPhones come with an extensive set of Restrictions or "parental controls". A Guide can either set these on an Explorer's phone or pay to use the kind of remote control software businesses use for their employee's iPhones[1]. I'll describe these two options in Restrictions: The Apple Way part I and II.

Android phones are different. They don't come with much in the way of built-in restriction software. Guides need to pay to use a parent-oriented software that works like the software Guides and Explorers use. I'll describe one option I've evaluated called MMGuardian in Restrictions: The Google Way.

Restrictions: The Apple Way I

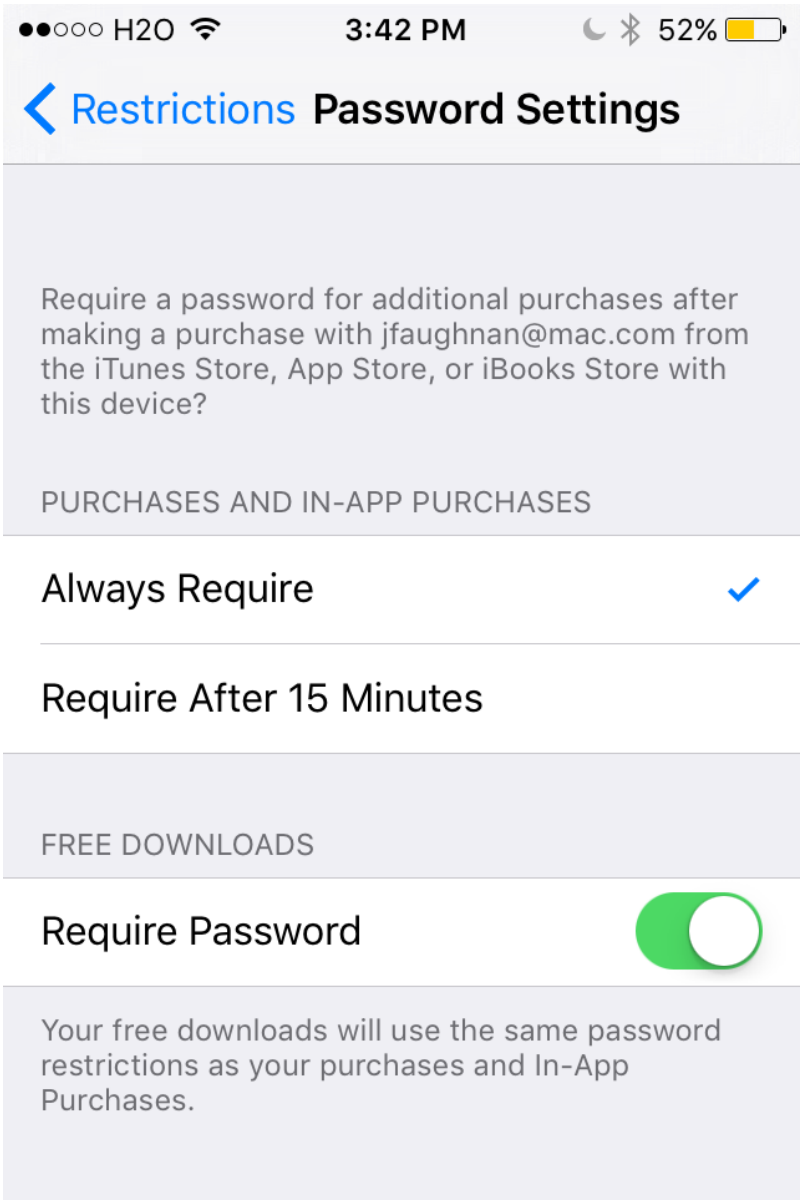
iPhone Guides have two ways to manage restrictions for an Explorer. One way is free but configuration requires physical control of an Explorer's phone. The other option requires signing up with an online service and typically costs around $20 a year. I'll discuss the free options here and the remote management service in the next section.

The standard option for iPhone users is briefly described in the User Guide, but Apple put most of the documentation on using Restrictions into a support note[2]. A Guide will want to spend some time familiarizing themselves with what's possible. This support document also references a related document on managing password preferences[3].

Using these documents as a guide the first step is to configure the Explorer's password preferences. For most Explorers I recommend software installation and removal be done by the Guide - at least to start with. If the Explorer's iPhone has Touch ID then it should be enabled for the phone (see Setting up an Explorer's Smartphone) but not for iTunes and App Store[4].

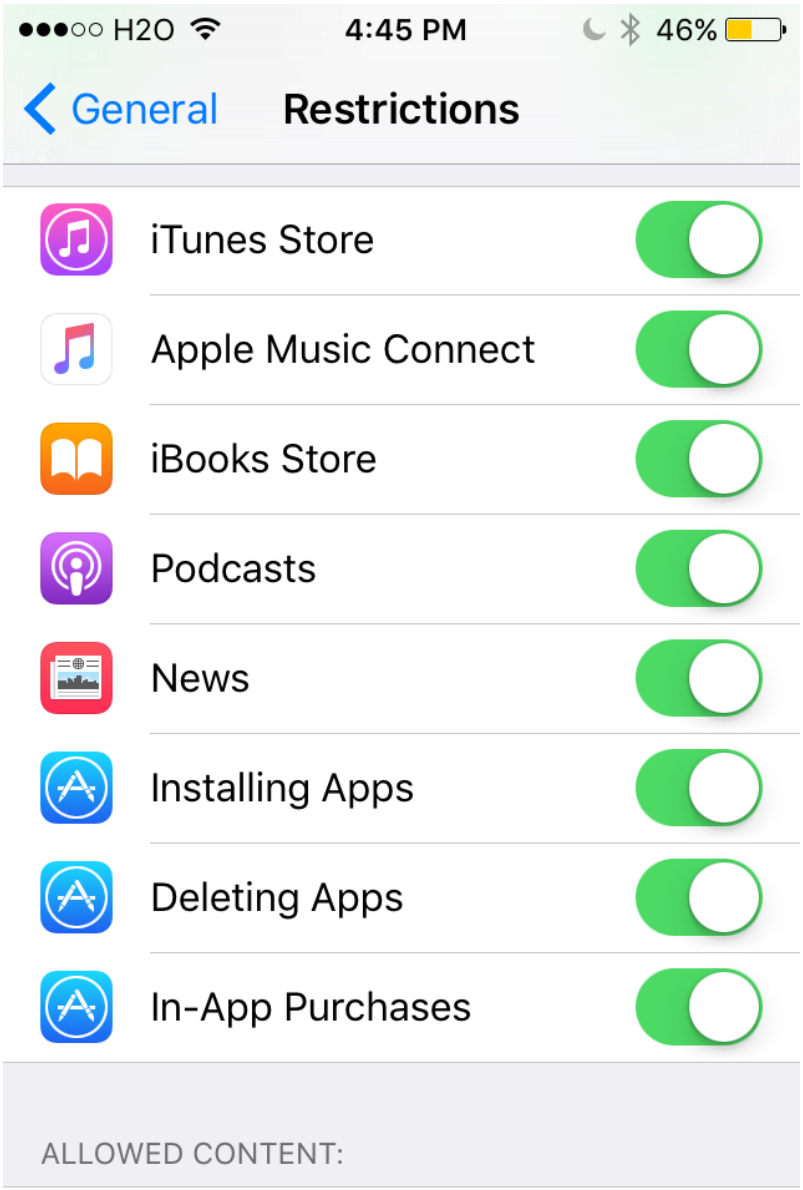
The next step is to enable Restrictions as described in the User Guide or the support document I referenced. The Guide will need to create a Restrictions passcode only they know. Don't lose this (See Credentials: usernames and passwords)! There's no way to recover a lost Restrictions passcode, the phone would need to be wiped and reconfigured.

Once Restrictions are enabled the Guide will tap Settings > General > Restrictions > Password Settings and and choose "Always Require" and "Require Password":



The Password in this case is the iTunes store password, I reviewed this in Setting up an Explorer's smartphone: iPhone. An Explorer who is less than "Step 5" will not know this password, so even if they can browse the App Store or iTunes Store they can't complete a purchase. This is a key step.

A Guide can next decide if they wish to enable App Store and iTunes Store browsing and App deletion. There are settings for these in the Restrictions menu. It's a good idea to allow App Store browsing, because disallowing it may prevent App updates. The screenshot below shows settings for an Explorer who can browse the iTunes Store (music, videos, etc) and the App Store ("Installing Apps" should really be labeled "App Store"), and can also delete apps. Some Explorers delete Apps a Guide may want to keep; there are no issues with turning "Deleting Apps" off.



Apple's support document has a good description of other restrictions. Here are some of the ones to pay special attention to in addition to those discussed above. They're organized below by Apple's section headings.

ALLOW

- **Safari**: For Step 1 you will turn this off. For more advanced levels this is on, but another setting will limit what web pages appear.
- **iTunes Store**: If an Explorer's phone is configured to require a password for purchases, including free downloads, then the main reason to turn this off is to prevent browsing the iTunes Store. I usually leave it on.
- **App Store**: If an Explorer's phone is configured to require a password for purchases, including free downloads, then the main reason to turn this off is to prevent browsing the App Store. Turning it off may prevent updates to apps

though. I recommend leaving this on.

- **iBooks, Podcasts and News**: For some Explorers these may too distracting. Podcasts in particular can be exotic. I turn these off if I know of a specific issue or if I need to reduce complexity.

ALLOWED CONTENT

- **Music, Movies etc**: This is where you can set ratings thresholds like "TV-14" or "PG-13". One of the choices here is "Don't Allow"; that will completely hide Movies or TV Shows.
- Websites: See below.

PRIVACY

These can be used to restrict access of third party apps to the personal information. I usually leave these alone, but I'm cautious about installing 3rd party apps. It's good to review these and turn off any surprises.

ALLOW CHANGES

These can be used to prevent an Explorer from changing settings. They can be annoying to use, you need to go elsewhere to set things like Volume Limit, then come here to prevent Explorer changes.

- Accounts: Guide may lock this if unwanted changes are a problem. I usually leave this alone.
- Cellular Data Use: This can prevent changes to the Cellular settings. See Controlling data use for how to use the Cellular settings. I only use this if an Explorer is changing the Cellular settings despite my warnings.
- Volume Limit: Prevents changes to a volume limit setting.

GAME CENTER

I always turn these off. I don't feel I can monitor these interactions well enough.

Of all these settings the ALLOWED CONTENT for Websites will be most important for many Explorers. If you include the Safari on/off setting there are 4 choices related to web access:

- Safari Off: This means no web access at all unless a different browser is installed. This is Step 1 on the 5 step progression.
- Specific Websites Only: A Guide must authorize each new web site using the Restriction code. This is tedious at first, but for many Explorers additions slow after the first 20 or so. It works well. This matches Step 2 and 3 on the 5 step progression.
- Limit Adult Content: In my experience this is pretty similar to no limits at all. It's a Step 4 and 5 choice.
- All Website: this is a Step 5 choice.

Restrictions: The Apple Way II

We've seen that Apple's iPhones come with a lot of Restriction options that a Guide can setup on an Explorer's iPhone. But what if the iPhone isn't at hand?

Fortunately schools and businesses have to manage business phones that aren't at hand, so Apple built a solution for them to use. It's called Mobile Device Management or MDM. MDM is the only option for Android phones, but it's a choice for Apple phones.

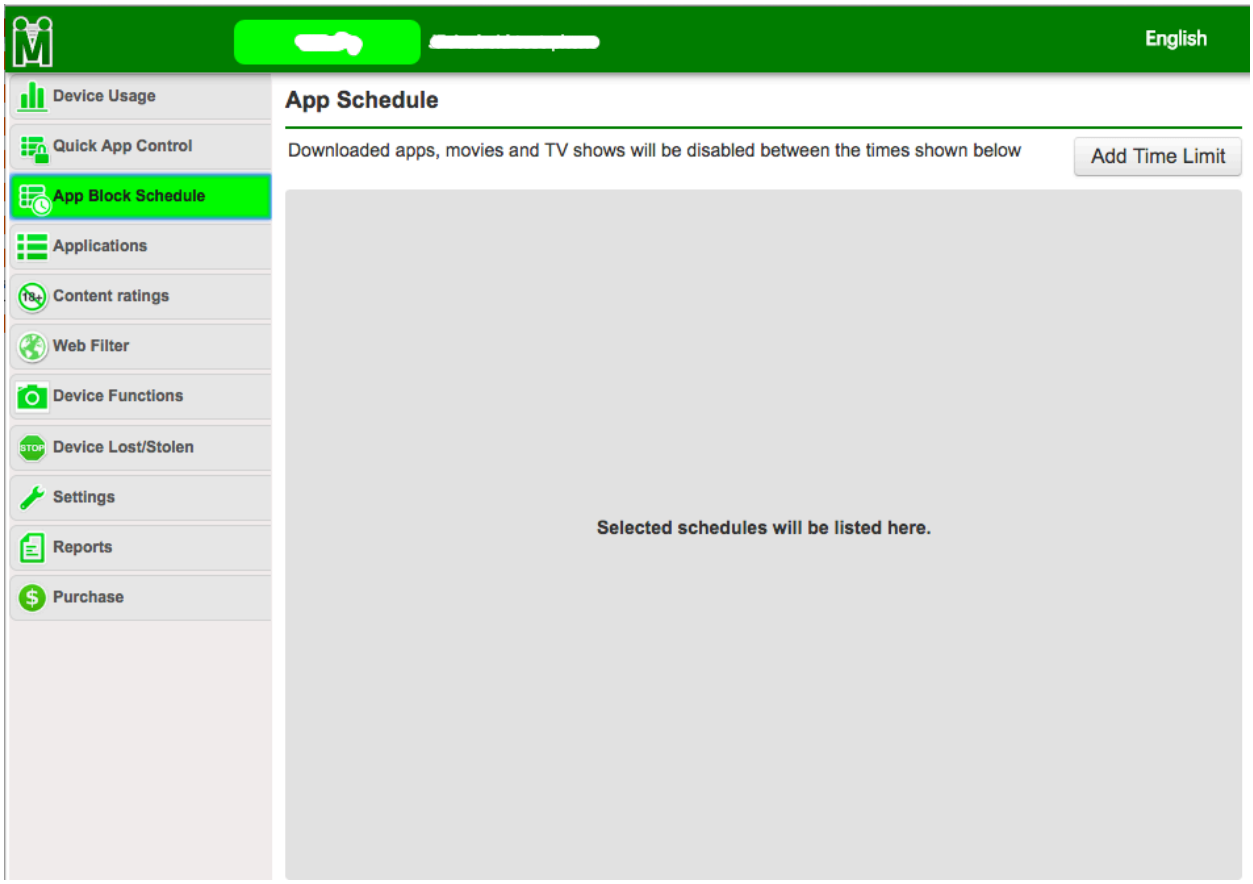
There are several businesses that provide these remote management services for consumers, typically for parents managing their children's phones using a web browser or a phone app. These services can also be used for a Guide managing a teen or adult Explorer's phone.

They vary in quality, cost and features. After evaluating several options I focused on MMGuardian[5]. Qustodio[6] is a newer service with similar cost and features, it looks like a worthy alternative.

MMGuardian currently costs $2 to try it for a month (be sure to turn auto-renew off in the App Store!), if you like it you can pay $20 for a year for each device. MMGuardian isn't perfect. There are a few bugs and awkward screens and it's a bit tricky to install. More annoyingly the documentation doesn't tell you how to uninstall MMGuardian! The developers don't want children to know that deleting the "Management Profile" from an Explorer's phone removes remote control — so they want customers to request uninstall directions by email.

If your Explorer does delete the Management Profile you'll receive an email notice. This might be a chance to discuss options, such as more restrictive controls directly on the phone versus more permissive controls with MMGuardian use.[7]

The screenshot below shows a typical MMGuardian screen. Most of the restrictions I've reviewed are available under the headings on the left.



MMGuardian provides more advanced web filtering options than the native iPhone restrictions, but they require use of the MMGuardian web browser. That MMGuardian browser is installed on the Explorer's phone and the Safari browser is hidden.

MMGuardian restrictions can be combined with phone based restrictions, but the resulting behaviors are a bit hard to understand. It's usually better do one or the other, but not both. One exception is using MMGuardian for all restrictions except web content; that way an Explorer can continue to use the Safari browser.

Restrictions: The Google Way

When it comes to restriction options the Apple Way and the Google Way are quite different.

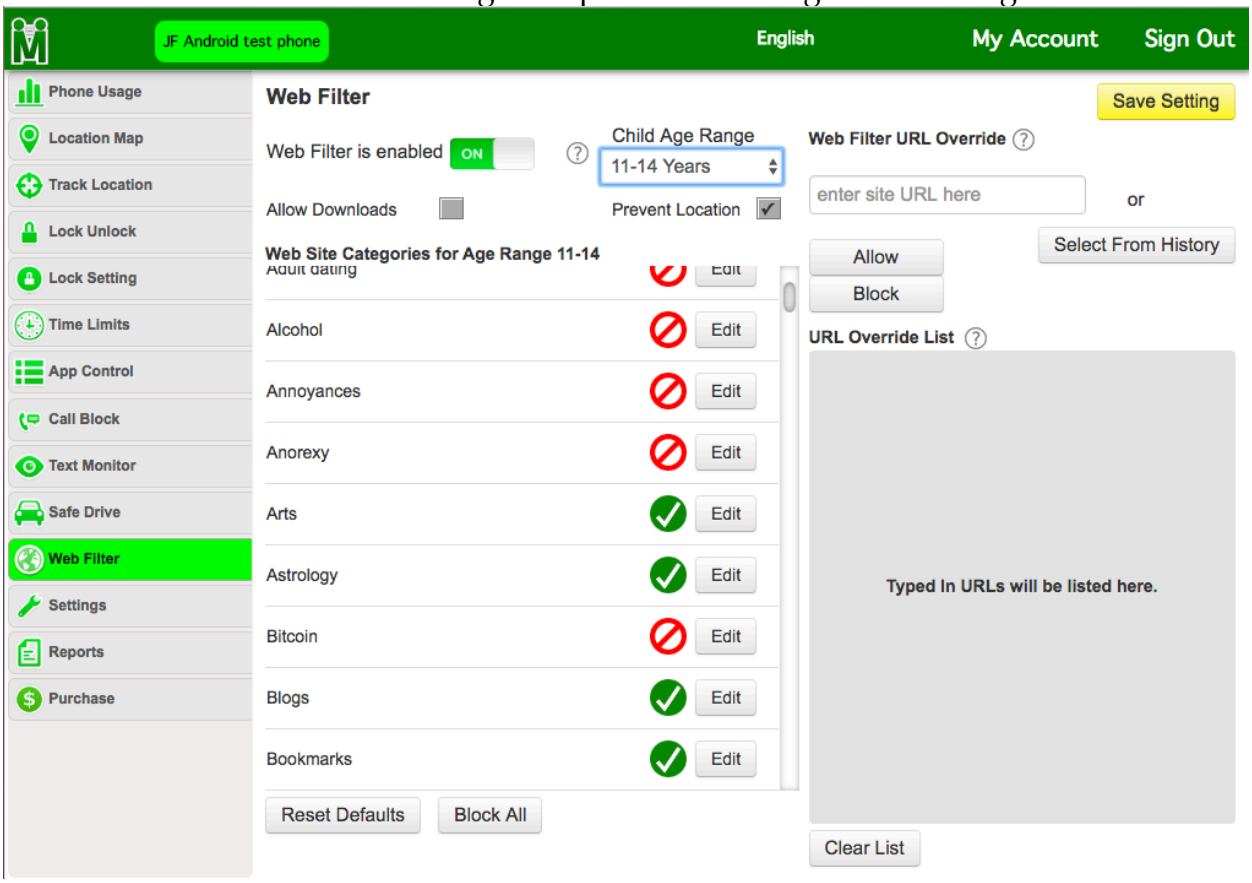
Apple supports restriction either set directly on an iPhone or set remotely using "Mobile Device Management" software. Google's Android phones have only the Mobile Device Management option. The good news is that Android's remote management options are more powerful than their iPhone equivalents.

For Android Guides, as for parents of children using Android phones, this means paying for consumer oriented Mobile Device Management services. There are some

ad-supported "free" options for Android, but after reviewing several alternatives, including Screen Time, Net Nanny and Norton Family, I liked MMGuardian[8]. It costs $50 a year for a single Android device, $70 for up to 5. There's a 14 day free trial and you can also opt for 1 month at a time ($4, auto-renews).

I was also impressed by Qustodio (www.qustodio.com), a hard to spell service that markets to schools and businesses as well as families. Qustodio charges $50/year for up to five devices which can be Android, iPhone or even laptops.

A Guide begins by installing the MMGuardian control software and MMGuardian Browser on the Explorer's phone. After that restrictions can be managed remotely including disabling apps, setting time controls, preventing app installation, monitoring texting, and scheduling locations and blocking calls. The screenshot below shows the range of options including web filtering.



Screen abuse - a special concern

I know what it's like to spend too much time staring at my screens. I love being outside and doing things, but I still get pulled into the virtual world. That pull can be stronger for Explorers who may have fewer outside interests. Explorers on the autism spectrum may be particularly prone to extreme screen use; use that can interfere with personal development, social relationships, health, and work.

Compulsive screen use that interferes with health and work is often compared to substance or gambling addictions. The similarities are obvious, but I think these comparisons are misleading. Gambling, for example, isn't an essential activity. There aren't a lot of negative effects to never gambling or never using alcohol. Screen use isn't like that — it's hard to work and live in the modern world without using a smartphone or other computer.

I think a better analogy is to compare screen overuse to overeating. We all have to use screens, we all have to eat. In the modern world we have an abundance of very tasty and inexpensive food, and almost everyone struggles to eat less of it. People who love to exercise have an easier time with weight control, but most of us weigh more than we like.

If we think about screen abuse the way we think of overeating then we think differently about management. We need to manage our diet and we need to manage screen time; we need to balance both eating and screen time with other activities.

Of course we all now how hard it is to manage diet. Everyone can lose weight on a restricted diet of healthy foods, but for most of us that would require a diet enforcer. That's not available for food. Happily, it is available for screen time — at least for an Explorer with a Guide.

With the restrictions I've described a Guide can turn a smartphone into the digital equivalent of a carrot and broccoli diet. Nobody will abuse a "Step 1" smartphone that has Calendar and Contacts but no messaging or games or web access. Using restrictions a Guide and Explorer can work together the find the right balance between fun and work. For example, each week an Explorer could choose a single game to install on their smartphone. Web access can likewise be limited to a selected set of useful but dull web sites. With MMGuardian time limits can be set for application use on either iPhone or Android devices.

Smartphone restrictions make screen diets much more effective than food diets. They can be adjusted to match other activities an Explorer wants to purse; work and exercise might earn more recreational screen time. The goal over time is for the Explorer to take on more management of their screen time. That development may take years of work but it's work that's well supported by restriction tools. If only diets came with those…

Beyond restrictions: learning safe practices

As an Explorer progresses from Step 1 (limited phone) towards Step 5 (independence) they get the same spam everyone gets. They get emails and Facebook messages that appear to be from friends who need money, from stranded royalty with money to share, and from attractive "women[9]" or lonely men seeking

partners. They are tricked into installing malware or divulging passwords. Elderly people are prime targets for most online criminals, but so are many Explorers.

It's a rough world out there. Even technically sophisticated experts can be tricked by modern "phishing" attacks that trick users into divulging passwords or installing malware. Everyone has to learn that "too good to be true" is a good rule and that exciting stories are often inventions.

The Explorer has advantages however. Caution and suspicion is more a matter of temperament than academic ability — many Explorers have a native caution to build on. As a Guide monitors progression from Step 1 and up many "teachable moments" arise. A Facebook connection to an attractive stranger can removed from an Explorer's account, but it can also used to teach about common frauds. Since Explorer emails are monitored (See Email and creating a digital identity) scams that make it through modern filters can be caught by Guides and used as examples.

If a Guide follows the advice in The Guide's Toolbox an Explorer won't know their passwords. You can't be tricked into revealing something you don't know.

Lastly Explorers are primarily using smartphones, not traditional computers. Modern smartphones are much more secure than older computers, iPhones in particular are effectively free of malware. (Android phones are less secure). They are also more likely to be backed up (See Setting up an Explorer's Smartphone). If, as I recommend, an early stage Explorer doesn't have the ability to install software they can't be tricked into installing a malicious application.

Between native caution and formal support from a Guide the Explorer is probably less vulnerable than many peers, and has time to become well equipped for independent life in a sometimes unfriendly world.

---

[1] In business and school settings this is called "mobile device management" or MDM.

[2] https://support.apple.com/en-us/HT201304

[3] https://support.apple.com/en-us/HT204030

[4] With iOS 9 this is under Settings: Touch ID and Passcode.

[5] http://www.mmguardian.com/

[6] https://www.qustodio.com/en/family/premium/

[7] There's currently no way for MMGuardian or others to prevent Management Profile deletion. Apple chose to give users this ability.

[8] http://www.mmguardian.com/

[9] In net frauds the "women" are always men and the "men" are always men.