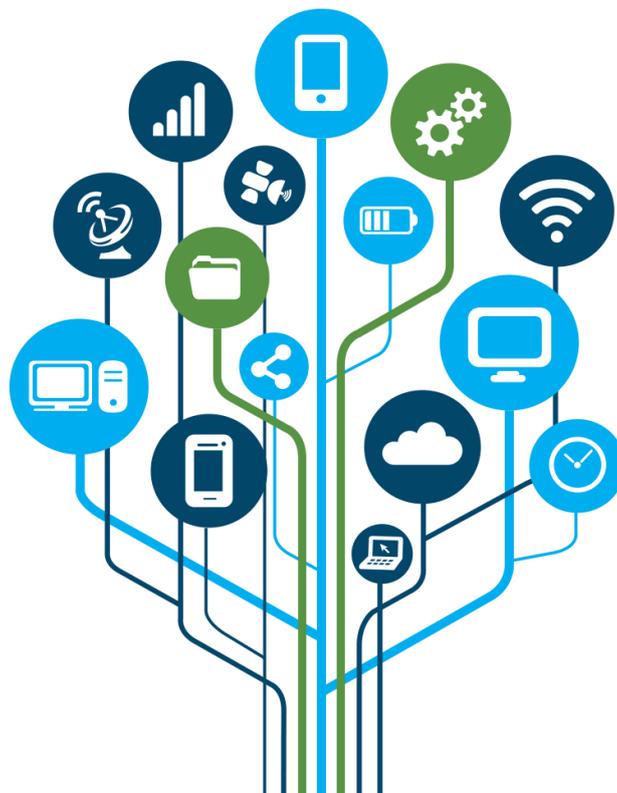# Christian Values in Education

SCREEN SAFETY AND SECURITY: A PRACTICAL GUIDE

RESOURCE PACK

Revision 1.0: 10/09/2018

CONTENTS

INTRODUCTION

Our children grow up with technology and the Internet all around them. At CViE, we have received multiple requests for help from parents who wish to protect their children online and manage their use of technology, but do not know where to start.

The only certain way of protecting your children is to keep them offline and away from computers and mobile devices. However, in the 21st century context, especially in the world of education, this is more or less impossible and so it is important to consider what can realistically be done.

In response to this need, we have developed a number of Screen Safety and Security resources to assist parents:

1. A CViE leaflet *Screen Safety and Security: A Practical Guide* provides a high-level overview of the topic and identifies 10 key tools and topics to consider.
2. This resource pack has been produced to supplement the *Screen Safety and Security: A Practical Guide* leaflet by providing more in-depth information and links to other external resources.
3. A webpage that contains all the above information – www.cvie.org.uk/resources/screen-safety-security.

It is important to clarify a few points at this stage:

- ✓ The intention of the leaflet and this resource pack is to assist parents with making informed decisions about how they and their families use and think about technology.
- ✓ It is not our role or intention to dictate a specific approach. We hope the resources are useful, but please use them as a starting point for your own research.
- ✓ Whilst this leaflet summarises 10 key practical things to think about, it is unlikely that you will need to use them all. Please decide for yourself on the best approach for your family and your circumstances.
- ✓ We at CViE are by no means experts in this field. As such, we are not presenting anything new here, but rather have produced a signpost or road map to resources and information already available elsewhere.

We pray that the resources in this pack will be useful. As with all things, we need wisdom in navigating a path through these challenging topics. As such we are thankful to remember God's promise to us that '*If any of you lack wisdom, let him ask of God, that giveth to all men liberally, and upbraideth not; and it shall be given him.*' (James 1:5)

KEY RESOURCES

There are several key online resources from which much of the information in this pack is taken. These are:

https://www.internetmatters.org/

https://www.net-aware.org.uk/

Christian Values
in Education

https://www.saferinternet.org.uk/

Whilst these sites provide excellent advice and resources, it should be noted that they are all secular in nature and should be used with discernment.

POTENTIAL RISKS

It is worth briefly setting the scene by considering why it is important to engage with this topic and to keep informed. To do this we'll summarise some of the key risks and dangers children may face on electronic devices, the Internet and when using social media:

✓ Accessing inappropriate content – sexually explicit content (including pornography, and films/TV shows), gory & violent content, drug related content, gambling etc.
✓ Spending too much time on devices or online – addiction to social media, online games etc., loss of sleep.
✓ Chatting with strangers, grooming etc.
✓ Sharing personal information in an uncontrolled fashion.
✓ Sharing inappropriate personal information / images (e.g. sexting).
✓ Sharing location information.
✓ Cyber-bullying, peer pressure, image pressures, struggling with low self-esteem etc.
✓ Influence of advertising.

These can be summarised in four 'Cs' as outlined by UK Safer Internet Centre[1]:

✓ Conduct: children may be at risk because of their own behaviour, for example, by sharing too much information, or spending too long online.
✓ Content: age-inappropriate or unreliable content can be available to children.
✓ Contact: children can be contacted by bullies or people who groom or seek to abuse them, children can become obsessed with needing validation from their 'friends' (e.g. craving likes and shares).
✓ Commercialism: young people can be unaware of hidden costs and advertising in apps, games and websites.

A BALANCED VIEW OF TECHNOLOGY

When considering the dangers outlined in the Potential Risks section above, it is tempting to panic and think that the world of smartphones, technology and the Internet is no place for children and young people. However, a balance approach is needed.

Few would claim that the widespread use of technology has been entirely beneficial to individuals or society. Equally, few would deny that technology and the Internet has also brought great benefits.

It is easy to think that *'the former days were better than these'*, but we are told in Ecclesiastes 7v10 *'for thou dost not inquire wisely concerning this'*. Down through the ages God has given man the wisdom to invent different forms of communication and we should be careful about questioning His providence in providing us

---

[1] UK Safer Internet Centre – What are the Issues? - https://www.saferInternet.org.uk/advice-centre/parents-and-carers/what-are-issues

with the latest advances in technology.

Johann Gutenberg, the inventor of the printing press, said: '*Through it God will spread his Word. A spring of pure truth shall flow from it! Like a new star, it shall scatter the darkness of ignorance, and cause a light heretofore unknown to shine among men*'.

Much good has indeed come from the printing press, but also much evil. The same can be said for the Internet and modern forms of communication. Easy access to useful information is countered by pornography and other evils. The benefits of instant communication are offset by the addictive nature of smartphones and the negative impact of excessive usage on our wellbeing. Simple sharing with family and friends is undermined by selfish, image-obsessed attitudes and problems with self-esteem and bullying.

The section above was called 'potential risks', precisely because the risks outlined can be mitigated. If we put in place sensible controls, coupled with training our children about how to use technology wisely and how to behave sensibly online, then the dangers can be minimised.

Technology is a tool. It's not inherently wrong in and of itself - if we use it rightly it can be of help and profit, whereas if we use it wrongly it can do great harm both to ourselves and others. Therefore, whether young or old, we should prayerfully seek God's help to use technology wisely.

LEAFLET / RESOURCE PACK STRUCTURE

Within the leaflet and this resource pack we have focused our practical tools and suggestions on three areas:

- ✓ Content: managing what is accessed.
- ✓ Time: managing when and for how long.
- ✓ Social media: managing interactions with others.

For each of these, the tools vary depending on the type of Internet connection (WiFi / Mobile Data) and the type of device (desktop PC or laptop / smartphone or tablet). Further variations are then added dependant on the make of device and the software installed on it.

Within the leaflet *Screen Safety and Security: A Practical Guide,* a grid shows which tools / resources to consider for different applications & scenarios. This is summarised as 10 practical hints, tips and tools.

1. DISCUSS WITH YOUR CHILDREN
2. SET-UP ISP FILTERS
3. SET-UP MOBILE FILTERS
4. SET-UP WEB BROWSER FILTERS
5. SET-UP MOBILE DEVICE CONTROLS
6. PASSWORD PROTECT APP STORES
7. LIMIT PHONES/TABLETS TO WIFI
8. INSTALL THIRD PARTY SOFTWARE
9. OPERATING SYSTEM SETTINGS
10. THINK ABOUT SOCIAL MEDIA

In the remainder of this resource pack these are covered in greater detail, with links provided to external resources.

PRACTICAL TOOLS

Each colour coded section below covers one of the 10 practical tools identified in the *Screen Safety and Security: A Practical Guide* leaflet.

1 – DISCUSS WITH YOUR CHILDREN

Don't just rely on technology to protect technology!

This is relevant to all circumstances and practical setups. It is also perhaps the most important step in keeping your children safe online.

As parents we are responsible for **what** technology we allow into our home and **when** that can be used, but our children will choose **how** and **why** they will interact with it. The Bible tells us to '*train up a child in the way he should go*' (Proverbs 22:6) Therefore it is crucial that we interact with our children on this topic, talking to them about it, teaching and guiding them. The Biblical principles outlined in the *Screen Safety and Security: A Practical Guide* can be helpful here.

It is important to reiterate that CViE is not here to tell you how to bring up your children. However, we have prepared some suggested conversation topics that may be useful:

- ✓ Help children to understand dangers they face on the web, and with the different apps and devices they use.
- ✓ Tell them your expectations; what you consider suitable online behaviour.
- ✓ Explain which filters and safety devices are in place and your reasons for implementing these.
- ✓ Explain why time limits are in place and why they are important.
- ✓ Seek to understand what your children really want to do online, what apps they wish to use etc. This may differ from what you thought.
- ✓ Encourage your children to talk to you about any concerns or issues they have.

Having this type of conversation helps build up a trusting relationship that will be invaluable in keeping your children safe on the Internet. It's also worth remembering that with many aspects of this topic, your children probably know more than you do and therefore may also be able to help keep you informed and up to date!

Another resource you may find useful is the Childnet Family Agreement. This provides templates and advice for having technology discussions with your children. It can be found here:

- ✓ https://www.childnet.com/resources/family-agreement

A final thought here: if we implement rules and boundaries with our children, it is also important where possible to keep to them ourselves and to be consistent in our own online habits. We should all challenge ourselves…are we setting a good example to our children?

2 – SET-UP ISP FILTERS

- ✓ Filters are available at the Internet Service Providers' (ISP) level and can be activated for the broadband connection into your home.
- ✓ These filter the broadband coming into your home to block access to adult and illegal content.
- ✓ The filters use blacklists of restricted sites and automatically block pages by examining keywords to determine whether a site should be prohibited.
- ✓ This blocking (or filtering) happens at the network level so it does not rely on software on your devices or hardware in your home.
- ✓ It is applied to your entire Internet connection, so filtering works on any device connected to your home broadband network (whether hardwired or via WiFi).

✓ The key advantage for parents is that they don't need to worry about configuring settings on every bit of hardware that has a web browser. Whether your child is using a smartphone, tablet, games console or computer, the filtering can prevent them accessing unsuitable sites.

✓ NOTE: This does not provide filtering on devices connected to the Internet via a mobile data (3G / 4G / 5G) connection. For the equivalent for mobile data networks see section 3.

The table below provides links to help pages for setting up these filters for all the main ISPs:

BT	✓ https://www.internetmatters.org/controls/interactive-guide/BT/ ✓ http://bt.custhelp.com/app/answers/detail/a_id/46768/~/bt-parental-controls---'how-to...'-guide#settingup
sky	✓ https://www.internetmatters.org/controls/interactive-guide/Sky/ ✓ http://www.sky.com/shop/broadband-talk/broadband-shield/
TalkTalk	✓ https://www.internetmatters.org/controls/interactive-guide/TalkTalk/ ✓ https://help2.talktalk.co.uk/how-use-talktalk-homesafe%C2%AE
Virgin media	✓ https://www.internetmatters.org/controls/interactive-guide/Virgin-Media/ ✓ https://my.virginmedia.com/customer-news/articles/online-safety.html
plusnet	✓ https://www.internetmatters.org/parental-controls/broandband-mobile-networks/plusnet-safeguard/ ✓ https://www.plus.net/help/archive/other/plusnet-protect-user-guide/?supportarchive

3 – SET-UP MOBILE FILTERS

✓ Filters can be set up at the mobile network level for controlling content accessed via a mobile data network (3G / 4G / 5G).

✓ How this is done varies between mobile network providers and should be done with your provider.

✓ The mobile networks do not utilise the same blocks as home ISPs but rather use guidelines developed by the BBFC (British Board of Film Classification), which classifies sites on a similar basis to an 18-rated film – filtering out sexually explicit, gory, violent, and drug related content.

The table below provides links to help pages for setting up these filters for all the main network providers:

EE	✓ https://www.internetmatters.org/controls/interactive-guide/EE/ ✓ http://ee.co.uk/help/help-new/safety-and-security/content-lock/switching-content-lock-on-or-off
O2	✓ https://www.internetmatters.org/controls/interactive-guide/O2/ ✓ https://www.o2.co.uk/help/everything-else/digital-family/the-internet
vodafone	✓ https://www.internetmatters.org/controls/interactive-guide/Vodafone/ ✓ http://www.vodafone.com/content/digital-parenting.html/howto-guides/vodafone_content_controls.html

3	✓ https://www.internetmatters.org/controls/interactive-guide/3/ ✓ http://support.three.co.uk/SRVS/CGI-BIN/WEBISAPI.DLL?Command=New,Kb=Mobile,Ts=Mobile,T=Article,varset_cat=intern-etapps,varset_subcat=3582,Case=obj(16080)
TESCO mobile	✓ https://www.internetmatters.org/controls/interactive-guide/Tesco-Mobile/ ✓ https://www.tescomobile.com/help-and-support/1812-safety-and-security/1815-parental-controls
Virgin media	✓ https://www.internetmatters.org/controls/interactive-guide/Virgin-Mobile/ ✓ https://help.virginmedia.com/system/templates/selfservice/vm/help/customer/locale/en-GB/portal/200300000001000
TalkTalk	✓ https://www.internetmatters.org/controls/interactive-guide/TalkTalk-Mobile/ ✓ https://help2.talktalk.co.uk/about-mobile-parental-controls

4 – SET-UP BUILT IN WEB-BROWSER / SEARCH ENGINE CONTROLS

✓ A web-browser is the program or software you use to access the Internet.
✓ Examples include Internet Explorer, Edge, Chrome, Firefox, Safari etc.
✓ A search engine is a tool used to find content on the Internet. The most well-known are Google and Microsoft's Bing.
✓ Advice for setting up controls on these can be found here:
  ➢ https://www.internetmatters.org/parental-controls/entertainment-search-engines/

5 – SET-UP BUILT IN CONTROLS ON MOBILE DEVICES / OPERATING SYSTEMS

✓ An operating system is the on-screen interface on your desktop computer, laptop or mobile device.
✓ In this section we are considering operating system settings on mobile devices. For the equivalent for desktop computers and laptops see Section 9.
✓ The main mobile operating systems are Android and iOS (Apple devices).
✓ These controls allow the parent to set up which apps and features are available, and what content can be accessed.
✓ Note: These controls do not allow time restrictions to be implemented. For this functionality third party apps can be used (see Section 8).
✓ Note: It is also possible to disable location services on mobile devices so that children do not inadvertently share where they are, however this may also prevent you seeing where they are should you use tracking apps.

The table below provides links to help pages for setting up parental controls on the main mobile operating systems.

ANDROID	✓ https://www.internetmatters.org/parental-controls/devices/android-smartphone/ ✓ https://www.teamknowhow.com/kit-guide/phones/android/how-to-set-up-android-parental-controls

iPhone	✓ https://www.internetmatters.org/parental-controls/devices/apple-iphone/ ✓ https://www.teamknowhow.com/kit-guide/phones/apple/iphone-7/iphone-parental-controls ✓ https://support.apple.com/en-us/HT201304
amazon	✓ https://www.internetmatters.org/parental-controls/devices/amazon-fire-hd/

6 – PASSWORD PROTECT APP STORES

- ✓ This is linked closely with Section 5.
- ✓ App Stores are the places you go to buy and / or download apps. Apps are pieces of software for mobile devices.
- ✓ Many apps are free to download but include in-app purchases.
- ✓ You can set up passwords on mobile devices to restrict which apps can be used and to prevent purchases without authorisation.
- ✓ The table in Section 5 provides links to help pages for setting up parental controls on the two main mobile operating systems – these include settings for restricting purchases.

7 – LIMIT SMARTPHONES AND TABLETS TO WIFI

- ✓ This is linked closely with Section 5.
- ✓ Mobile devices such as smartphones and tablets can connect to the Internet via a mobile data network (3G / 4G / 5G) or via WiFi.
- ✓ It is possible to restrict them to just WiFi which can make filtering content easier.
- ✓ Note: Restricting access to the mobile data network will not prevent a phone being used for calls / text messages.
- ✓ For details on how to restrict Internet access to just WiFi consult the user manual for your particular device. These can usually be found with a quick Internet search.

8 – THIRD PARTY APPS

- ✓ A wide variety of third party apps and software is available across the different platforms and device types to enhance screen safety and security.
- ✓ Some of these are free, others charge.
- ✓ They each have different functions and you should do your own research to ensure any software you use fulfils your own specific requirements.
- ✓ The table below provides a brief overview of some of the main options. Note this is not a comprehensive list.

Qustodio	https://www.qustodio.com/en/
Qustodio provides content filtering and time management across multiple devices / platforms. It has some interesting features such as allowing you to restrict time spent on specific apps on specific days. Qustodio is available on a variety of paid plans dependent on how many devices you wish to protect. Feedback suggests that Qustodio may not work so well with older Apple devices or versions of iOS.	
OurPact	https://ourpact.com/

OurPact provides content filtering and time management across multiple devices / platforms. It also allows you to see the location of your child's device. OurPact has quite a powerful free plan, but for the full complement of features you will require one of the paid plans.

(Net Nanny logo)	https://www.netnanny.com/

NetNanny provides content filtering and time management across multiple devices / platforms. It also allows social media usage to be monitored. NetNanny is available on a variety of paid plans dependent on how many devices you wish to protect, although for maximum flexibility across multiple platforms the cheapest plan will not be suitable.

(Kaspersky Safe Kids logo)	https://www.kaspersky.co.uk/safe-kids

Kaspersky Safe Kids provides content filtering and time management across multiple devices / platforms. It also allows you to see the location of your child's device and manage some social media usage. Kaspersky Safe Kids is available as a variety of paid plans dependent on how many devices you wish to protect.

(CovenantEyes logo)	https://www.covenanteyes.com/

Covenant Eyes is slightly different from the other software outlined above. It is more focused on those battling with pornography, providing accountability and content filtering. It is available across multiple platforms and devices. It does not provide time management features. Covenant Eyes has a number of paid plans but does work out quite expensive compared to some other options.

9 - OPERATING SYSTEM SETTINGS (MAINLY FOR PCS AND LAPTOPS)

- ✓ An operating system is the on-screen interface on your desktop computer, laptop or mobile device.
- ✓ In this section we are considering operating system settings on desktop computers and laptops. For the equivalent for mobile devices see Section 5.
- ✓ Unlike ISP filters (Section 2) and mobile data filters (Section 3) which just filter content, these operating system controls allow you to control access to apps and games, and to set limits for screen time.
- ✓ Logs can also be maintained of computer usage and websites visited. This can then be emailed weekly to the parent and child, promoting responsible use.
- ✓ One point to note here is that it is important for your children to have their own operating system account / login. It may seem that this means parents lose a level of control, however it is in fact the exact opposite. It is much easier to control a child's account, than it is to control a child on your own account.

The table below provides links to help pages for the two main desktop / laptop operating system:

(Windows logo)	✓ https://www.teamknowhow.com/kit-guide/computing/laptops/dell/inspiron-13-5000/how-to-set-up-parental-controls-in-windows-10 ✓ https://support.microsoft.com/en-gb/help/17199/windows-10-set-up-your-family

- ✓ https://www.teamknowhow.com/kit-guide/computing/laptops/apple/macbook-pro-13-with-retina-display-(2015)/macos-osx-parental-controls
- ✓ https://support.apple.com/kb/PH25799?locale=en_GB

10 – THINK ABOUT SOCIAL MEDIA

- ✓ A dictionary definition of social media is '*Websites and applications that enable users to create and share content or to participate in social networking*'.
- ✓ There are a host of social media platforms, the most well-known being Facebook and Twitter. However, for today's teens, these are being replaced by Instagram, YouTube, SnapChat etc.
- ✓ Social media platform all have a minimum age restriction. This is usually 13, although WhatsApp have recently increased the minimum age to 16.
- ✓ Communicating via online multiplayer games is also widespread. One of the most popular of these amongst teenagers (and adults) is Fortnite.
- ✓ Whether we think it is right for our children to participate in any form of social media or other form of communication is a decision for parents, and what may be suitable for some families may not be suitable for others.
- ✓ The Internet Matters and NetAware websites once again provide much useful information on different social media and chatting apps. Here are links to these:
  - o https://www.internetmatters.org/advice/apps-guide/
  - o https://www.net-aware.org.uk/
  - o https://smartsocial.com/app-guide-parents-teachers/
- ✓ A useful article on sites popular with teens is:
  - o https://www.commonsensemedia.org/blog/16-apps-and-websites-kids-are-heading-to-after-facebook

The table below provides links to further information regarding the most popular social media apps in the UK for young people. **Note: this is rapidly and constantly changing. It also varies hugely in different parts of the country and in different social groups.**

	Instagram is a picture and video sharing app. Users can post content and use hashtags to share experiences, thoughts or memories with an online community. ✓ https://www.net-aware.org.uk/networks/instagram/ ✓ https://www.internetmatters.org/hub/guidance/instagram-safety-a-how-to-guide-for-parents/ ✓ https://help.instagram.com/154475974694511/
	Snapchat is an app that lets you send a photo, short video or message to your contacts. The 'snap' appears on screen for up to 10 seconds before disappearing. ✓ https://www.net-aware.org.uk/networks/snapchat/ ✓ https://www.internetmatters.org/hub/guidance/snapchat-safety-a-how-to-guide-for-parents/ ✓ https://www.snapchat.com/l/en-gb/safety/

	Facebook allows you to share personal information, status updates, pictures, videos and chat with a network ✓ https://www.net-aware.org.uk/networks/facebook/ ✓ https://www.facebook.com/safety/
	YouTube allows you to watch, create and comment on videos. You can create your own YouTube account, playlists and channel with a public profile. ✓ https://www.net-aware.org.uk/networks/youtube/ ✓ https://www.internetmatters.org/controls/interactive-guide/YouTube/ ✓ https://support.google.com/youtube/answer/174084?hl=en-GB
	WhatsApp is an instant messaging app which lets you send messages, images and videos in one to one and group chats ✓ https://www.net-aware.org.uk/networks/whatsapp/ ✓ https://www.internetmatters.org/hub/guidance/whatsapp-safety-a-how-to-guide-for-parents/ ✓ https://faq.whatsapp.com/en/general/21197244
	Google Hangouts is an app that lets you video call, phone or message other users. You can either speak to one person at a time or have group conversations. ✓ https://www.net-aware.org.uk/networks/google-hangouts/
	Twitter is a messaging service that lets you post public messages called 'tweets' up to 280 characters long. You can also send private messages and post pictures/videos. ✓ https://www.net-aware.org.uk/networks/twitter/ ✓ https://about.twitter.com/en_gb/safety.html
	KiK is an instant messaging app that allows you to create your own username, share messages, photos, games and news, or organise events. ✓ https://www.net-aware.org.uk/networks/kik/ ✓ https://www.kik.com/safety-center/
	Tumblr is a social networking site that lets you share text, photos, quotes, links, audio clips, slideshows and videos. You can customise your page and share other people's posts. You can also send private messages. Tumblr allows live streaming. ✓ https://www.net-aware.org.uk/networks/tumblr/
	ASKfm is a social networking site where you can ask other people questions. You can choose to ask the question anonymously. ✓ https://safety.ask.fm/parents-guide-to-ask-fm/
	Fortnite is a multi-player online battle game. ✓ https://www.net-aware.org.uk/news/fortnite-all-you-need-know/ ✓ https://www.childnet.com/parents-and-carers/hot-topics/gaming