SCREEN SAFETY & SECURITY
A PRACTICAL GUIDE

CONTENTS:

INTRODUCTION

This leaflet has been prepared by Christian Values in Education in response to feedback from parents requesting information on the tools available to assist with managing screen safety & security. Intentionally high-level, it provides an overview of general background, Biblical principles and practical hints, tips & tools, whilst signposting to detailed information and resources elsewhere. Three main areas are considered:

✓ Content Management
✓ Time Management
✓ Social Media

A BALANCED APPROACH TO TECHNOLOGY

Our children grow up with technology all around them. It appears in many forms, both in the educational setting and in the home. There are differing views on the impact of this. Few would claim that the widespread use of technology has been entirely beneficial to individuals or society. Equally, few would deny that technology 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 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 well-being. Simple sharing with family and friends is undermined by selfish, image obsessed attitudes and problems with self-esteem and bullying.

In reality, technology is a tool. It's not inherently wrong in itself - if used rightly it can be of help and profit, whilst if used 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.


BIBLICAL PRINCIPLES

Although the Bible doesn't talk specifically about computers, smartphones, the internet or social media, it does give us clear principles which are very applicable to how we use technology in the 21st century:

DO EVERYTHING FOR THE GLORY OF GOD (1 Corinthians 10:31; Colossians 3:17)

✓ **AVOID LOOKING AT SINFUL MATERIAL (Psalm 101:3-4; Psalm 119:37; Romans 6:12-15)**

✓ **BEWARE OF FALSE INFORMATION (1 John 4:1; Colossians 2:8; 1 Timothy 6:20)**

✓ **FOCUS ON GOOD THINGS (Philippians 4:8; 2 Corinthians 8:21)**

✓ **BEWARE OF MIXING WITH THE WORLD TOO MUCH (Romans 12:1-2; 1 John 2:15-17)**

✓ **SPEND THE TIME WE HAVE BEEN GIVEN WISELY AND USEFULLY (Ephesians 5:15-16; Colossians 3:23)**

✓ **EXERCISE SELF-CONTROL (Proverbs 25:28; Galatians 5:23; 2 Peter 1:6)**

✓ **TAKE CARE HOW AND WHAT WE COMMUNICATE (1 Corinthians 15:33; Psalm 141:3; Ephesians 4:25)**

These Biblical principles can be used to guide how we think about technology usage in a general sense and more specifically with how we seek to help and protect our children. However, it is also worth taking the time to challenge ourselves personally with them - are our own actions and habits glorifying God and consistently setting the right example to our children and others around us?
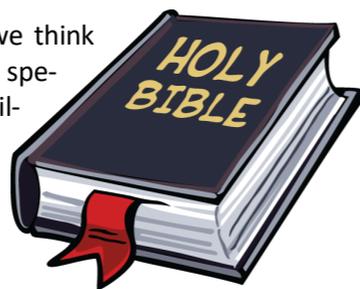
PRACTICAL TOOLS CHECKLIST

This checklist summarises the various hints and tools. The most effective approach to eSafety will depend on individual circumstances, but is likely to involve a mixture of these. Use the reference numbers to find further information in the Screen Safety Resource Pack which can be downloaded at cvie.org.uk/resources/screen-safety-security.

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

CONVERSATIONS ARE IMPORTANT

Don't just rely on technology to protect technology!

The Bible tells us to 'train up a child in the way he should go' (Proverbs 22:6). Therefore a key aspect of screen safety is talking with your children about it. We're not here to tell you how to bring up your children, but here are 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.

✓ Encourage your children to talk to you about any concerns or issues they have.

Having this type of conversation can 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 be able to help keep you informed and up to date!

CONCLUSION

We are conscious that each individual will take a different approach to protecting their children online. However, we hope and pray that this leaflet will prove a helpful starting point.

When considering such a vast and rapidly changing subject it is encouraging to remember that God and His Word never change. We are thankful that we can turn to him for wisdom and guidance in all things.

'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)

Christian Values in Education

www.cvie.org.uk   christianvaluesineducation

ACCESSING THE INTERNET

Whether browsing websites, accessing social media platforms, or using other apps, a connection to the internet is required.

This is true both on desktop computers and **mobile devices** such as smartphones and tablets.

There are two main ways of accessing the internet (as summarised in the diagram below right):

✓ Via a broadband connection and a wireless (**WiFi**) network.

✓ Via a mobile data network (**3G / 4G / 5G**) usually from a **mobile provider**.

Different approaches must be taken to ensure screen safety and security dependent on how you are connecting to the internet and which type of device you are using.

The different approaches required and the various tools available are outlined in the *Practical Tools* section of this leaflet.

THREE KEY AREAS

In this leaflet we are considering three key aspects of eSafety—tools and strategies for managing:
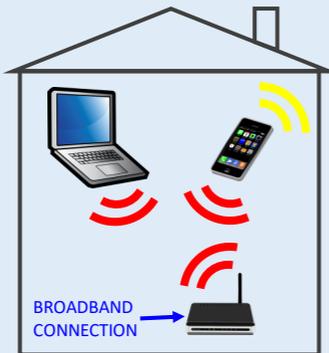
Content, what is accessed.

Time, when and for how long.

Social Media, interactions with others.

BROADBAND CONNECTION

Wireless Network (WiFi) - Internet access within approx. 20m of the access point (WiFi router)

3G / 4G / 5G - Internet access via the mobile network wherever there is mobile reception.

DESKTOP / WiFi

MOBILE (3G / 4G / 5G)

1 Be aware of the key issues with eSafety and discuss these with your children. Talk through with them why filters & safety devices are in place and what they do. Make sure they know what you consider suitable online behaviour, and your reasons why.

2 Set up **ISPs** filtering options. This is done at the network level so does not rely on software or hardware in your home and will protect all devices using your broadband (e.g. computer, smartphone, games console). Note: **Mobile devices** accessing the internet via **3G/4G/5G** will not be protected.

3 Set up filters from **mobile providers**. These use guidelines developed by the British Board of Film Classification to classify websites on a similar basis to 18-rated films – looking for sexually explicit, gory, violent & drug related content. Note: Filters must be set up on each device and vary between providers.

4 Consider only having one **web browser** on your computer and ensure that built-in safe search settings, content filters and age limits are set up on this. Also set up controls on the major search engines. Note: **Operating system** settings can also be used to control what content is accessed (see '9').

5 Set up any built in parental controls on your child's **mobile device**, (see also '6' and '7').

6 Password protect **app stores** on Phones and Tablets to restrict what is downloaded.

7 Phones & tablets can be set up to only access the web via **WiFi** which allows content to be more easily managed.

8 Consider installing third party software/**apps** to manage both content and time across all devices. Many options are available, each with varying features, so doing your research is important to ensure you get what you require.

Qustodio   OurPact   Net Nanny   Kaspersky Safe Kids   CovenantEyes

9 Configure family settings or a family account on your **operating system** (Windows, Apple etc.) for each child. This will enable you to set time boundaries and limits of when your children can be online, as well as filtering content. You can monitor activity whenever you want and receive weekly reports.

✓ Neither Android nor Apple mobile **operating systems** have built in screen time controls (although they do have content filters), so use third party apps (see '8').
✓ Consider limiting mobile devices usage to communal areas and set clear time boundaries (e.g. not at meal times or late at night).

10 All the above tools can help to monitor and manage **social media** use. However, there are also some specific points to consider, including:
✓ Ensuring social media accounts are set to private so that your children really have to think about who they want to be friends with.
✓ Ensuring your children are aware of the dangers of sharing private or personal information and images with people they do not know.
✓ Ensuring your children are aware that everything they post could be permanent and cause future implications or embarrassment.

PRACTICAL TOOLS

✓ The grid above summarises practical hints, tips and tools for managing **Content**, **Time** & **Social Media** across different operating systems, networks and types of device. The colour coded reference number links to the checklist on the back page and to further details in the more comprehensive Resources Pack available on the CViE website - see: cvie.org.uk/resources/screen-safety-security

✓ Other useful resources are the Internet Matters (internetmatters.org), Net Aware (net-aware.org.uk) & UK Safer Internet Centre (saferinternet.org.uk) websites which are great starting points for more in depth information.

✓ Note: In this leaflet we do not look at the potential dangers of technology - for a summary see the separate Resource Pack.

GLOSSARY OF TERMS

3G / 4G / 5G - Different types of mobile network. The most significant difference is speed.

APP - Short for 'Application' - a piece of software on a mobile device.

APP STORE - The online shop where apps are purchased / downloaded.

ISP (INTERNET SERVICE PROVIDER) - The company you buy your home broadband from (e.g. BT, TalkTalk etc.)

MOBILE PROVIDER - The company you buy your mobile phone service from (e.g. EE, O2, etc.)

MOBILE DEVICE - A smartphone or tablet. For the purpose of this leaflet, laptops are not counted as mobile devices.

OPERATING SYSTEM - The on-screen user interface on your computer or mobile device (e.g. Windows, iOS, Android etc.)

SOCIAL MEDIA - web-based apps for creating and sharing content (e.g. Facebook, Twitter, Instagram, YouTube, Foursquare, Periscope, Snapchat etc.). Can also cover multi-player online games.

WEB BROWSER - The program you use to access the internet (Chrome, Edge, Internet Explorer, etc.)

WiFi - A wireless internet connection.