# The Royal Alexandra and Albert School

# E Safety Advice for Parents

# Contents



# Introduction

The Internet is a wonderful and diverse place, filled with incredible information resources. Yet for many parents and careers, who often have less knowledge and experience of the Internet, it can be a place of concern. We worry about what or whom our children may encounter online, and how we can protect them with our own limited knowledge.

While we use it for booking holidays and answering emails, your children are setting up social networking pages, instant messaging with webcams, blogging, researching school projects, listening to music, playing online games and emailing friends.

Most children use the internet safely and responsibly and we shouldn't therefore lose sight of the positive aspects. As parents, we need to balance our concerns about their safety online with empowering them to explore and make the most of this wonderfully rich resource, safe in the knowledge that they can talk to us about anything they may run into.

In clear, simple language, this booklet explains to parents what children already know or need to know about the online environment as well as providing advice about how you can protect your family, allowing them to use the Internet safely and securely while having as much fun as possible.

# E Safety at RAAS

We take the safety of our pupils very seriously and endeavor to ensure they have the best experience online that they can. To do this all devices connected to our network or Wi-Fi have age appropriate filters that ensure inappropriate content cannot be accessed. We also have down times set up on the Wi-Fi system so that at age appropriate times the Wi-Fi no longer works for pupils to allow them to go to bed and not worry about social media.

We also have a piece of software that takes screen shots of any inappropriate use of the internet by pupils. These are checked on a daily basis and pupils that have tried to access inappropriate material are then helped to understand what they have done and how to correctly use the internet in the future.

We give regular assemblies to all the pupils about this area of life to help them think about how they use the internet and how they could improve this use. These cover a wide range of topics related to E-Safety and can change dependent on current issues we are finding.

We do expect all parents to place age appropriate filters and restrictions on any personal devices that their child brings onto the school site. This is to ensure that any 4/5G internet connections are also filtered so that pupils cannot get onto inappropriate material or apps. Any device that is found not to have these restrictions will be confiscated and returned to the parent the next time the parent is on the school site.

# Top Tips for Parents

1. Set up an account for each user on your PC at home and only give yourself administrator access. This will allow you to keep control of the settings and the installation of software. Each user account can be password protected. You can do this in the 'Control Panel'.

2. Add a screen saver protected by a password to your account so that if you leave the PC for 5 minutes you will have to enter your password. You can do this in the 'Control Panel'.

3. Encourage your family to use technology in a public part of the house, and **not** in the bedroom, where it's easier to monitor what your children are doing. This applies not just to PCs but also to laptops and games consoles. If a predator sees a living room/kitchen in the background on the webcam rather than a child's bedroom, they will be less likely to embark on attempting to groom your child.

4. Remember that many games consoles come with family settings. For example, if you want to disable or limit 'Xbox Live' on the Xbox 360 you can do so by going to 'Settings, Parental controls'. There is also the option to add a mask to voices so that a youngster's voice sounds like that of an adult or even a robot. See the 'Online Gaming and Games Consoles' section for further information.

5. Encourage your child not to open emails from unfamiliar email addresses and to avoid opening suspicious attachments. As far as possible you should encourage your child to use the school's email system and Learning Platform as this provides a safer environment.

6. Set your favorite search engine to do 'safe searches'. This will make sure that a search returns content suitable for all ages. For example, to set Google to do safe searches click on search settings on the homepage and then ensure that moderate or strict filtering is enabled.

7. Tell children not to give out their personal details whilst online. If they want to subscribe to any online services or websites make up a family email address to receive the mail.

8. The internet is a great resource for homework, but remember to use more than one site in research to get broad, balanced information and always reference your research sources.

9. Involve your children in writing your own family code of 'Acceptable Computer & Internet Use'. Remember that what's acceptable for a teenager isn't necessarily ok for a primary school-aged child, so get their input. See the 'Activities for use at home' section.

10. Surf together and engage in their world. Go online with your child and become part of their online life – add them as friend on a social networking site (once they're old enough), text them and discover what their game consoles can do. Keep up...today's technology is tomorrow's antique!

# Social Networking and Instant Messenger

Social Networking sites are among the fastest growing phenomena on the Internet. Among the most popular social networking sites are Facebook, Twitter and Snapchat. All of them provide brilliant ways to stay in touch with friends and share photographs, comments or even play online applications. If used carelessly, however, they can expose you and your children to identity theft and online predators.

Instant messaging (IM) is a technology which enables you to send and receive messages almost instantaneously across an Internet connection. IM is much faster than email and is rapidly replacing the telephone as the primary method of a quick or instant communication. Examples of IM are: MSN, Windows Live, Yahoo!, and even Facebook has its own IM service.

Simple Social Networking and Instant Messenger Rules:

- ✓ Pay attention to age restrictions – for example Facebook and Bebo are only for people aged 13 years and older.

- ✓ Social networking sites, such as Facebook and Twitter, have a range of **privacy settings**. These are often setup by default to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a search engine, such as Google. So it is important to change your settings to 'Friends only' so that your details and profile content can only be seen by your invited and accepted friends and don't forget to remove yourself from search engine results.

- ✓ Have a neutral picture of yourself as your profile image. Don't post embarrassing material!

- ✓ You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may receive friendship requests or suggestions from people you do not know. It is not a competition to have as many friends as possible!

- ✓ You can delete unwanted 'friends' from you Social Networking sites and IM lists. On IM don't forget to 'Block' them as well so they can't request your friendship again.

- ✓ Exercise caution! For example in Facebook if you write on a friend's wall all their friends can see your comment – even if they are not your friend.

- ✓ If you or a friend are 'tagged' in an online photo album the whole photo album may be visible to their friends, your friends and anyone else tagged in the same album.

- ✓ You do not have to be friends with someone to be tagged in their photo album. If you are tagged in a photo you can remove the tag, but not the photo.

- ✓ Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.

# Social Networking and Instant Messenger

This is a very complicated area of people's digital life. These app or sites are continually changing and adding new versions and new functionality. Parents need to be very careful that they are happy that their child is not only mature enough to be able to use these appropriately but also physically old enough as set out in the companies' terms of use. The below are examples of current versions.

| Social Media | Icon | Terms of Use – Minimum Age Requirements | What is it? |
|---|---|---|---|
| ASK.fm | | 13+ | Ask.fm is an anonymous question and answer platform website |
| EA (Electronic Arts) | | 18+ (with parental permission up to 17 yrs) | EA is a digital distribution platform for multiplayer games. |
| Facebook | | 13+ | Facebook is a social networking website and service where users can post comments, share photographs and links to news or other interesting content on the Web, play games, chat live, and stream live video. |
| Facebook Messenger | | 13+ | Facebook Messenger is a social networking app made for texting and sharing photos and videos. |
| Flickr | | 13+ | Flickr is a photo sharing platform and social network where users upload photos for others to see. |
| Foursquare | | 13+ | This app helps you find new attractions or restaurants in your local area. It also allows friends to see your location. |
| Google+ | | 13+ | Google Plus is a social networking app made by google for sharing photos and videos. |
| Instagram | | 13+ | Instagram is a social networking app made for sharing photos and videos. |

| | | | |
|---|---|---|---|
| Keek | | 18+ (13+ with parental permission) | Keek is a video file sharing app. |
| Kik | | 18+ (13+ with parental permission) | Kik is a communication platform which allows text messaging and file sharing. |
| Linkedin | | 13+ | A professionals app that is built for linking to other professionals in similar sectors and also recruitment. |
| Minecraft | | All ages (parental permission required to create a mojang account if user is under 13 yrs) | A 3D construction game that has online chat. |
| Pinterest | | 13+ | A idea sharing app. Does contain inappropriate images and links. |
| Skype | | 18+ (13+ With parental permission) | Communication tool that allows voice, video and text messaging. |
| Snapchat | | 13+ | Snapchat is a messaging service that lets users send pictures & videos to one another, in the knowledge that such content will disappear after a set time. |
| Steam | | 13+ | Steam is a digital distribution platform for multiplayer games. |
| TikTok | | 13+ | Video sharing and lip-Sync App |

| | | | |
|---|---|---|---|
| Tinder | | 18+ (Facebook account required to register) | This is a dating site. |
| Tumblr | | 13+ | Tumblr is a free social networking website that allows registered users to post multimedia content to their own customizable blogs. |
| Twitter | | 13+ | A micro blogging site that allows users |
| Vine | | 17+ | Vines are short looping videos posted by members. |
| WhatsApp | | 16+ | Communication tool that allows voice, video and text messaging. |
| Whisper | | 17+ | Whisper is an anonymous social networking app. Users post confessions, either fact or fiction, by super imposing text on a picture. |
| Yubo (former Yellow) | | 13+ (With parental permission up to 17 yrs) | Yubo is a location based app that has similarities to adult dating sites. |
| YouTube | | 18+ (13+ With parental permission) | Youtube is a video hosting site. |

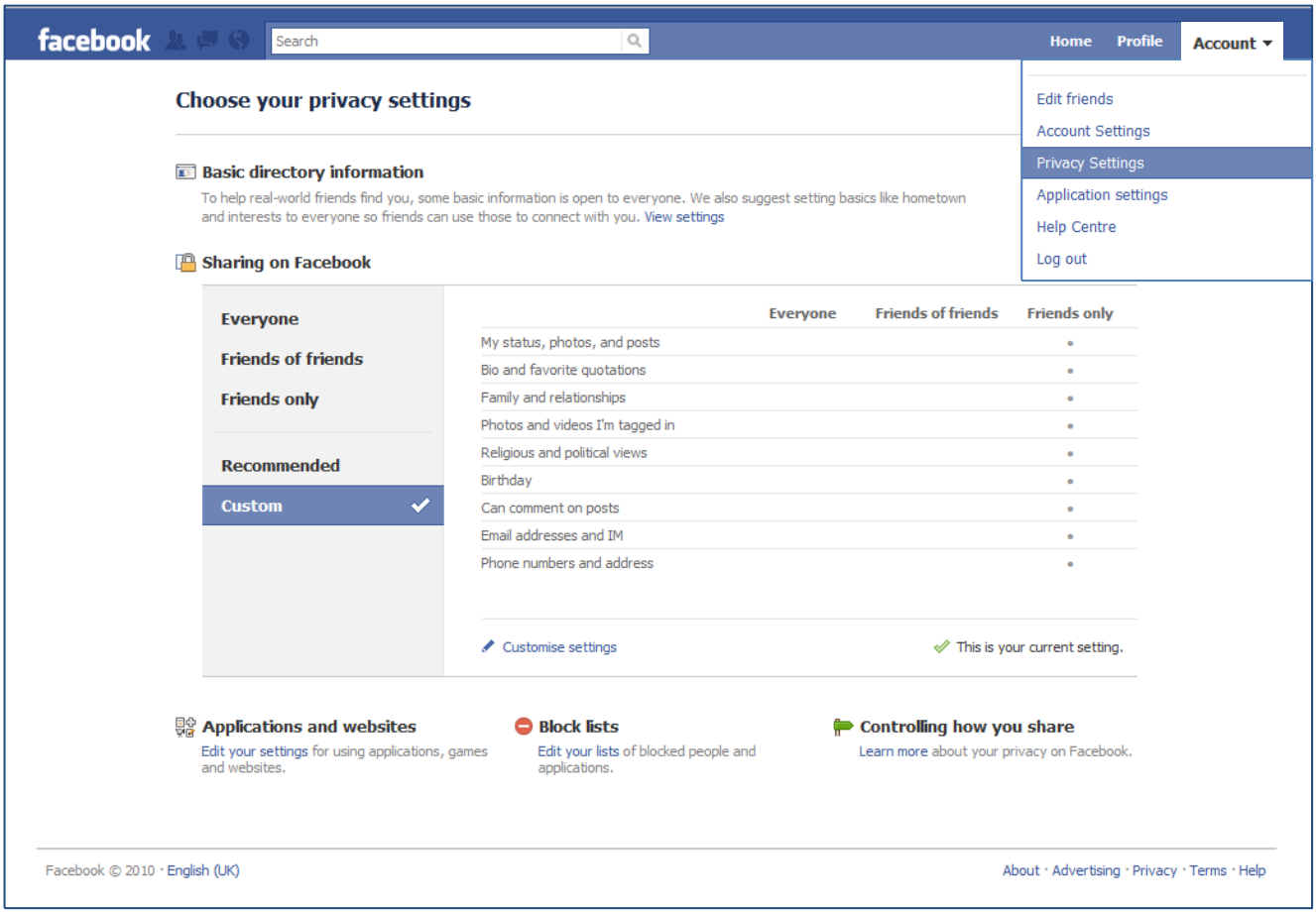
# Privacy Settings on Facebook

Facebook Privacy information can be found here:
http://www.facebook.com/home.php?#!/privacy/explanation.php

The safest way for your Facebook profile to be set-up is for it to be as private as possible i.e. only allowing your **Friends** to have access to your information and pictures. It is therefore advisable that you only have **REAL** friends as contacts on Facebook and other Social Networking sites.

Please see the image below of the ideal set-up for a Facebook profile. You can find this by following these steps:

1) Click on **Account** in the top right hand corner of your Facebook page.
2) Choose the **Privacy Settings** option.
3) You will then see the page below and you can edit the settings to ensure that **Friends only** have access to your profile and its information.



# Instant Messenger and Text Acronyms and Abbreviations

| | |
|---|---|
| **A3** | Anytime, anywhere, anyplace |
| **AAM** | As a matter of fact |
| **AB** | Ah bless |
| **ADctd2uv** | Addicted to love |
| **AFAIK** | As far as I know |
| **AFK** | Away from keyboard |
| **AKA** | Also known as |
| **ALlWansU** | All I want is you |
| **AML** | All my love |
| **ASAP** | As soon as possible |
| **ASL?** | Age, sex, location? |
| **ATB** | All the best |
| **ATK** | At the keyboard |
| **ATM** | At the moment |
| **ATW** | At the weekend |
| **AWHFY** | Are we having fun yet |
| **B4** | Before |
| **B4N** | Bye for now |
| **BAK** | Back at keyboard |
| **BBL** | Be back later |
| **BBS** | Be back soon |
| **BBSD** | Be back soon darling |
| **BCNU** | Be seein' you |
| **BF** | Boyfriend |
| **BFN/B4N** | Bye for now |
| **BGWM** | Be gentle with me |
| **BRB** | Be right back |
| **BRT** | Be right there |
| **BTW** | By the way |
| **CM** | Call me |
| **CU** | See You |
| **CUIMD** | See you in my dreams |
| **CUL** | See you later |
| **CUL8R** | See you later |
| **CYA** | See you |
| **DK** | Don't know |
| **DUR?** | Do you remember |
| **E2EG** | Ear to ear grin |
| **EOD** | End of discussion |
| **EOL** | End of lecture |
| **F?** | Friends |
| **F2F** | Face to face |
| **F2T** | Free to talk |
| **FAQ** | Frequently asked questions |
| **FC** | Fingers crossed |
| **FITB** | Fill in the blank |
| **FWIW** | For what it's worth |
| **FYA** | For your amusement |
| **FYEO** | For your eyes only |
| **FYI** | For your information |
| **G9** | Genius |
| **GAL** | Get a life |
| **GF** | Girlfriend |
| **GG** | Good game |
| **GMTA** | Great minds think alike |
| **GR8** | Great |
| **GSOH** | Good Salary, Own Home<br>Good Sense of Humour |
| **GTSY** | Glad to see you |
| **H&K** | Hugs and kisses |
| **H2CUS** | Hope to see you soon |
| **H8** | Hate |
| **HAGN** | Have a good night |
| **HAND** | Have a nice day |
| **IC** | I see |
| **ICQ** | I seek you |
| **IDK** | I don’t know |
| **ILU** | I love you |
| **IMBL** | It must be Love |
| **IMFL** | I'm Falling in Love |
| **IMI** | I mean it |
| **IMO** | In my opinion |
| **IOU** | I owe you |
| **IOW** | In other words... |
| **IRL** | In real life |
| **IUSS** | If you say so |

| | |
|---|---|
| **J4F** | Just for fun |
| **JFK** | Just for kicks |
| **KC** | Keep cool |
| **KHUF** | Know how you feel |
| **KISS** | Keep it simple, stupid |
| **KIT** | Keep in touch |
| **KOTC** | Kiss on the cheek |
| **KOTL** | Kiss on the lips |
| **L8** | Late |
| **L8r** | Later |
| **LDR** | Long distance relationship |
| **LMAO** | Laugh my ass off |
| **LOL** | Laugh out loud |
| **LTNC** | Long time no see |
| **M8** | Mate |
| **MOB** | Mobile |
| **MTE** | My thoughts exactly |
| **MYOB** | Mind your own business |
| **NA** | No access |
| **NC** | No comment |
| **NE** | Any |
| **NE1** | Anyone |
| **NO1** | No-one |
| **NRN** | No reply necessary |
| **NWO** | No way out |
| **O4U** | Only for you |
| **OIC** | Oh I see |
| **OTOH** | On the other hand |
| **PCM** | Please call me |
| **PITA** | Pain in the ass |
| **PPL** | People |
| **PRT** | Party |
| **PRW** | Parents Are Watching |
| **QT** | Cutie |
| **R** | Are |
| **RMB** | Ring my Bell |
| **ROFL** | Rolling On The Floor Laughing |
| **ROTFLMAO** | Rolling On The Floor Laughing My Ass Off |
| **RU?** | Are you? |
| **RUOK?** | Are you ok? |
| **SC** | Stay cool |
| **SETE** | Smiling ear to ear |
| **SK8** | Skate |
| **SME1** | Someone |
| **SO** | Significant other |
| **SOL** | Sooner or later |
| **SRY** | Sorry |
| **STATS** | Your sex and age |
| **SWALK** | Sent/Sealed with a loving Kiss |
| **T+** | Think positive |
| **T2Go** | Time to go |
| **T2ul** | Talk to you later |
| **TDTU** | Totally devoted to you |
| **THX** | Thank you |
| **THX40** | Thanks for nothing! |
| **TIC** | Tongue in cheek |
| **TMIY** | Take me I'm yours |
| **TTFN** | Ta-ta for now! |
| **TTYL** | Talk to you later |
| **U** | You |
| **U2** | You too |
| **U4E** | Yours forever |
| **UR** | You are |
| **URT1** | Your are the one |
| **W4u** | Waiting for you |
| **W8** | Wait... |
| **WAN2** | Want to |
| **WB** | Welcome back |
| **WLUMRyMe** | Will you marry Me? |
| **WTF** | What the f_ _ _ |
| **WTG** | Way to go! |
| **WUF** | Where are you from? |
| **WUWH** | Wish you were here |
| **X** | Kiss |
| **YBS** | You'll be Sorry |

# Online Gaming and Games Consoles

More than ever games are heading online. Everything from Scrabble to World of Warcraft can be played online and against other human opponents rather than computer controlled opponents, which can be a lot more fun. Players can usually communicate with one another; perhaps using onscreen messaging which is typed during the gameplay or some games allow voice communication so that players can swap their thoughts freely whilst competing just like a telephone conversation.

Today's games consoles can be a great way to bring the family together for endless hours of harmless fun. Whether it's bowling on the Nintendo Wii or Premier Manager on the Sony PlayStation, families can be involved in activity to develop communication and relationships.

The very best gaming however is safe gaming – which means games should be played responsibly. The ideal way to ensure that your children and teenagers are playing the right games, and playing sensibly, is to take an active interest in what they are playing.

Whether your children play on games a PC, Xbox 360, Nintendo Wii or Sony PlayStation, their gaming choices can be safely steered by you.

Play Safe Gaming Tips:

- ✓ ENGAGE – Find out what your children are playing and take an interest. Better still, join in the fun and play along yourself!

- ✓ LIGHTEN UP – Games should be played in well-lit rooms. Darkened rooms, where games are played on old TV sets, have been known to trigger epilepsy issues.

- ✓ TAKE BREAKS – Some games can be especially intense, so regular breaks are vital for healthy gameplay. Encourage your children to take regular breaks at least every 45 minutes.

- ✓ BE AWARE – Explain to your children how the online world differs from home or the school playground. Online your children will meet total strangers – some who may not be who they say they are. Often the chat will be uncensored, so they should be cautious about what they say and be careful not to give out private details such as their name, address, email address, passwords, telephone numbers or the name of their school.

- ✓ TAKE CONTROL – Take advantage of Parental Control setting available on your PC or games console. You can also decide which games are played by age rating and the PEGI descriptors or whether interaction which other games players is permitted at all.

For more information about online gaming visit: www.askaboutgames.com



# Games Consoles

On the PlayStation 3® guardians can set security levels to restrict access to games depending on age ratings. DVD and Blu-ray movies can also be blocked completely.

**To set security levels:**

1. To set game level, from the Main menu scroll across using the ⬅➡ to **Settings** and then down to **Security Settings**. Press ⊗ to select.
2. Scroll down to **Parental Controls** and press ⊗.
3. Enter your PIN Number then press ⊗ (the default PIN Number if you have not previously changed it is 0000).
4. Select required **Security Level** by scrolling from **Off** to **Levels 1-11**. Press ⊗ to confirm.
5. The following settings provide a guide corresponding with PEGI ratings:
   **2 –** PEGI 3+ **3 –** PEGI 7+ **5 –** PEGI 12+ **7 –** PEGI 16+ **9 –** PEGI 18+
6. The PIN can be changed from the **Security Settings** menu.

---

The XBOX 360® allows you to restrict access to games depending on a game's age classification. You can also add a timer, restricting just how long each day or weeks your children can play.

1. From the Main menu scroll across to the **System** tab on the right using ⬅➡.
2. Scroll down to the second option on this tab. **Family Settings** and press the **A** button to select.
3. Scroll on **Console Controls** and press **A**.
4. Enter your 4 digit pass code (if you haven't previously set a pass code you will need to set one on the **Control Consoles** menu by selecting **Set Pass Code**).
5. Scroll to **Games Ratings** and press **A**.
6. Now scroll to the age rating you wish to apply and press **A**. Users will eb able to play game sup to but not over this rating.

**To limit game splayed by time:**

1. Scroll to **Family Timer**, and on the **Console Controls** menu press **A**.
2. Scroll up and down to choose daily or weekly limits and press **A**.
3. Then scroll to the time bar ◀ **45 Minutes** ▶ and ⬅➡ to set usage time in minutes.
4. Scroll down to **Continue** and press **A**. Exit and save the settings by scrolling down to **Done** and press **A**. When you are asked if you wish to save the settings, scroll to **Yes**, save changes and press **A**.

---

The Wii™ allows you to restrict access to games depending on age classifications. But this console also allows parents the chance to limit online communication with others.

**To restrict game splayed by classification:**

1. Use the Wii remote to move the cursor over the Wii button in the bottom-left corner of the screen and press the **A** button.
2. Click on **Wii settings**.
3. Press the blue arrow ▶to reach the Wii System Settings 2 menu options.
4. Select **Parental Controls** and confirm.
5. Enter your 4-digit PIN in the white box (if you have not already set a PIN you will be prompted to do so now). Click **OK** and again to confirm.
6. Click on **Game Settings and PIN**.
7. Now adjust the Highest Game Rating Allowed by clicking on this option. On the menu that appears next, use the blue arrows ▲▼ to scroll to the desired setting. Once you have made your selection, hit **OK**. Click **Confirm** and then, on the next screen, **Settings Complete**.

## Grooming

Online grooming is:
'*A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes.'*
Sexual Offences Act, 2003

Often, adults who want to engage children in sexual acts, to talk to them for sexual gratification will seek out young people who desire friendship. They will often use a number of grooming techniques including building trust with the child in more intimate forms of communication, including compromising a child with the use of images and webcams. Child sex abusers will often use blackmail and guilt as methods of securing a meeting with a child.

How would I know if my child was being groomed?
There is no way of knowing without speaking to your child but there are some behaviours to look out for:

- → Excessive use of the computer.
- → Aggressive behaviour regarding internet usage.
- → Secretive behaviour.
- → Change in use of sexual language.

If you are concerned, talk to your child and review the sites they have been visiting regularly.

---

## Cyber Bullying

Technology gives our children more ways to connect, socialise, and communicate than ever before. Unfortunately, some children and young people use email, Instant Messaging, and mobile phone photos and text messages to embarrass or bully other children. Children's digital messages can also be edited to change the meaning then forwarded to others to embarrass, intimidate, or insult.

According to research carried out for the Anti-Bullying Alliance in the UK 22% of young people reported being the target of cyber bullying.

Make sure your children know they must guard even the most casual text message and watch their own written words. They should never retaliate, and they should always tell you if and when they are being cyber bullied.

Keep a copy of any bullying message received via a PC or laptop by using the "Print Screen" key on your computer keyboard and copying the message into a word processing program (e.g. Word). Likewise do not delete text messages or voicemails which also contain evidence of bullying.

## Computer and Online Security - Home

Computer viruses have been around for more than 25 years in various forms. But with the popularity of email and file exchange on the Internet, the distribution of these threats has really taken off. These days many of the bad guys are international cybercriminals, motivated by financial gain through their illegal activities.

Spreading via email, Instant Messaging, infected social networking pages, and file-sharing sites, malicious software (malware) such as spyware, keystroke loggers and bots can cause you enormous trouble.

Spyware and keystroke loggers monitor your normal computer activity and then report your private data out via the Internet to the criminals. Bots (short for robots) are forms of software that can sneak into your computer and cause your PC to send out spam and phishing emails to others, without you even knowing. Bots can also be used to steal your personal information and wreak havoc on your credit including the unauthorised use of your credit cards and bank accounts.

Help keep your children and your computers safe by installing Internet security software on your family's computers and making sure it's updated with the latest protection files. Tell your children not to turn off the virus scanner or firewall, even if they think it might speed up a game. It's just not a safe risk to take.

For more information visit: http://www.getsafeonline.org/

---

_

## Computer and Online Security - School

At school and in our boarding community we protect all users of our computer network by the following;

1. We have up to date virus and malware software running on every device and server to stop any virus, malware or spyware from moving onto the network. Any personal device that connects to our Wi-Fi network is also checked and must have similar software before it can fully connect.
2. We have a firewall installed that also blocks unwanted traffic. This system works by filtering traffic in both directions. The traffic that is out going is filtered to be age and time specific.
3. We also have software on the network that is continually monitoring all traffic for inappropriate content. This is based on keywords and other filters like skin tone. If something inappropriate is picked up a screen shot is taken and stored so that staff can discuss with the student. We use this to help to educate students so that they make the correct choices when being online. However, if further or serious incidents occur we do put in place sanctions or restrict or remove further access.

# Identity Theft

Many children will not automatically know what “private” information is and the importance of keeping this private both online and offline so you need to explain the concept that it’s any data that individually identifies them and may allow a stranger access to personal or financial information. Private information includes real world data such as, names, telephone numbers, addresses, sports club, school, even the name of a doctor.

Fraudsters can turn even a small clue into a full record on a child and parent. They, in turn, can trade and sell that private data to make money. It’s surprisingly easy for people with such intentions to apply for credit in your child’s name and get real world merchandise and money, while ruining the child’s (or your) credit rating and good name.

If you do suspect you’ve been a victim of identity theft, you are entitled to request a report from any of the credit reporting services for a small administrative fee: Equifax, Experian, and Callcredit all follow this. Once you find evidence of identity theft, you will need to report it to bank as soon as possible and you may also wish to discuss it with your local police force for advice and guidance. You can also put a “freeze” on your credit record and those of your children to prevent strangers applying for credit in your names.
For more information visit: http://www.ico.gov.uk

# Mobile Phones

You can now access the Internet on most mobile phones and whilst this access brings a world of incredible opportunities in terms of communication, interaction and entertainment, there are certain risks to children posed via the Internet. These risks include accessing potentially harmful content, such as pornography, possible dangerous contact with strangers in chatrooms and commercial pressures like spam and intrusive advertising.

The UK Mobile Operators have recognised these risks and have taken steps to help you protect your child from potentially harmful content accessible via your mobile phone. There are also things you can do to block premium rate calls and texts.

This guide written by children's internet charity, Childnet International, gives you a checklist of important questions to ask your Mobile Operator when purchasing a mobile phone so that you can ensure you have the tools and support to help protect children and make sure they get the most out of using their mobile phones safely.

| Questions to Ask | Background |
|---|---|
| **Safety Advice**<br>• Ask for information and advice about the phone and the services that are available on it, so that you can ensure your children know how to use it safely. | Your mobile operator is committed to providing you with information and advice on safe use of their service. Be sure to check that they are keeping you informed. |
| **Internet Access**<br>• Does this phone have internet access?<br>• Is there a filter to help block Internet content that is particularly harmful for children?<br>• Is the filter switched on? If no, can you switch it on please? | All the UK Mobile Operators have to provide an Internet filter on their phones to help block accessing material that is potentially harmful to children, such as pornography. However, with most operators you will need to ask your operator to activate the filter. |
| **Registering the Phone**<br>• Is the phone registered for a child or for an adult user? | Being registered as a child user will mean that you cannot access material provided by your mobile operator or its partners that is rated as 18+, i.e. unsuitable for children. |
| **Bluetooth-enabled Phones**<br>• Is this phone 'Bluetooth-enabled'?<br>• How can I turn this off, or set it so the phone is not visible to others? | Bluetooth technology essentially enables your mobile phone to find and 'talk' to other Bluetooth-enabled mobile phones in the vicinity, or other enabled phones to 'talk' to your mobile.<br>When activated on your child's mobile phone it means that they may receive unexpected and unwanted messages from other Bluetooth-enabled phone users nearby, and any personal information stored on your child's phone – for example their contact list – could be vulnerable. Switching off the Bluetooth option is safer as it makes the phone 'invisible' to other Bluetooth users. |

| Questions to Ask | Background |
|---|---|
| **Premium Rate Calls and Texts**<br>• Can you put a bar on all premium rate numbers?<br>• If you can't bar these numbers, what services do you provide to protect the user here? | If you do find you have signed up for a reverse-billed premium rate service (where you pay to receive rather than send text messages, e.g. for ringtones or football score updates) and you do not want to continue this, then text STOP to the shortcode number you got the text from. This will end the service and your payments to it. |
| **Chatrooms and Gaming**<br>• Can this phone access chatrooms or games where users can chat to each other?<br>• Are these chatrooms or games moderated?<br>• How are the chatrooms or games moderated? | Chatrooms or games (where you can chat to other users) what are provided by your mobile operator or its partners and which do not have an 18+ age-restriction must be moderated. |
| **Nuisance/Malicious Calls**<br>• What number can I call to report receiving unwanted or abusive calls or messages? | Your mobile operator should have systems and procedures in place to help you deal with nuisance and malicious phone calls. |
| **Reporting Abuse**<br>• Where do I report abuse of service? If for example I receive unwanted adult (18+) material on my phone while the filter is switched on, who should I report this to? | It is important to let your mobile operator know if their system is failing, both in order to protect yourself and others using the same service. |
| **SPAM**<br>• What action is your Mobile Operator taking to prevent SPAM? | Your mobile operator will take action against SPAM, whether it is text, picture or email. Find out what action your mobile operator is taking and report any SPAM received on your phone to them. |

## Mobile Phones in School and Boarding

We have restricted student use to mobile devices to allow students and teachers to concentrate on teaching and learning, and better social interaction. Boarders will register their devices with staff on their return and be allowed access to their devices for a period of time after school and before bedtime each weekday. At weekends, access is greater. All other students will be required to hand their devices in to the boarding house staff in the morning, should they bring any to school, and collect their devices when they leave the school site. If students decide to use a device it will be confiscated and returned at the end of the school day from their boarding house. After two incidents, parents will be contacted and required to collect the device from the boarding house. After three incidents the parent / carer will be required to collect the device from either the Assistant Head - Boarding or Head of School by appointment and should a fourth offence occur, the parent will be required to collect the device from a member of the Senior Leadership Team by appointment.

Before any student brings a mobile device into school or our boarding community we ask that parents / carers have set up parental restrictions on the device that are appropriate to the students age. We also ask that location software is installed and setup before the device comes onto our site so that the device can be found much more effectively if it goes missing.

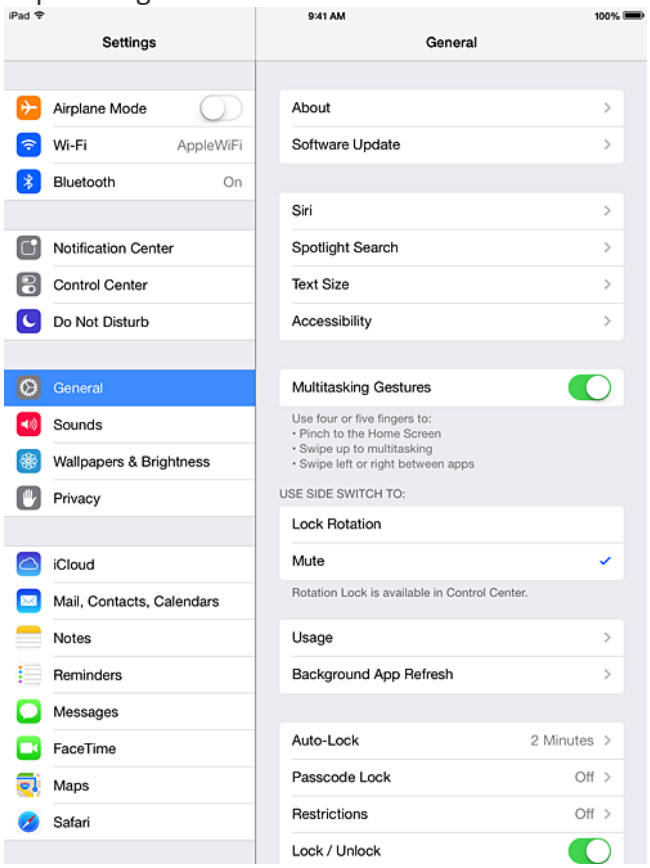
# Parental Restrictions - iOS

You can enable Restrictions, also known as parental controls, on iPhone, iPad, and iPod touch. Restrictions stop you from using specific features and applications. Learn more about the types of Restrictions and how to enable or disable them on your device.

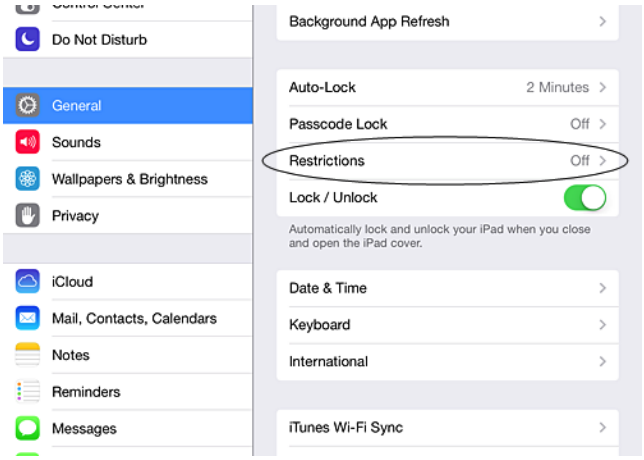
**Using Restrictions**

You can enable and adjust Restrictions on your device to prevent access to specific features or content on the device.

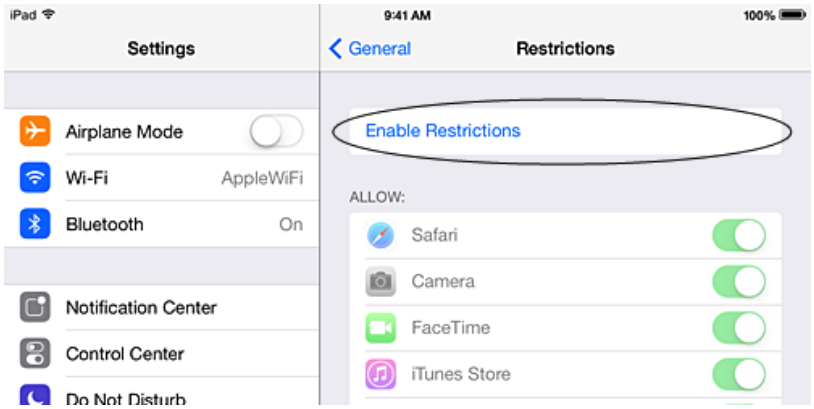
1. Tap Settings > General.




2. Tap Restrictions.



3. Tap Enable Restrictions and enter a passcode. You can use the passcode to change your settings or turn off Restrictions.
   **Important:** If you lose or forget your Restrictions passcode, you'll need to perform a factory restore to remove it.




You can restrict access to these applications and features on the device

- Safari
- Camera (also disables FaceTime)
- FaceTime
- iTunes Store
- iBooks Store
- In-App Purchases
- Siri
- AirDrop
- CarPlay
- Installing apps
- Deleting apps

You can prevent access to specific content types

- Ratings (select the country in the ratings section to automatically apply the appropriate content ratings for that region)
- Music and podcasts
- Movies
- TV shows
- Books
- Apps
- Siri
- Websites
- You can also adjust the time necessary before a password is required to purchase content

You can prevent changes to privacy settings, including

- Location Services
- Contacts
- Calendars
- Reminders
- Photos

- Bluetooth sharing
- Microphone
- Twitter
- Facebook
- Advertising

You can prevent changes to these settings and accounts

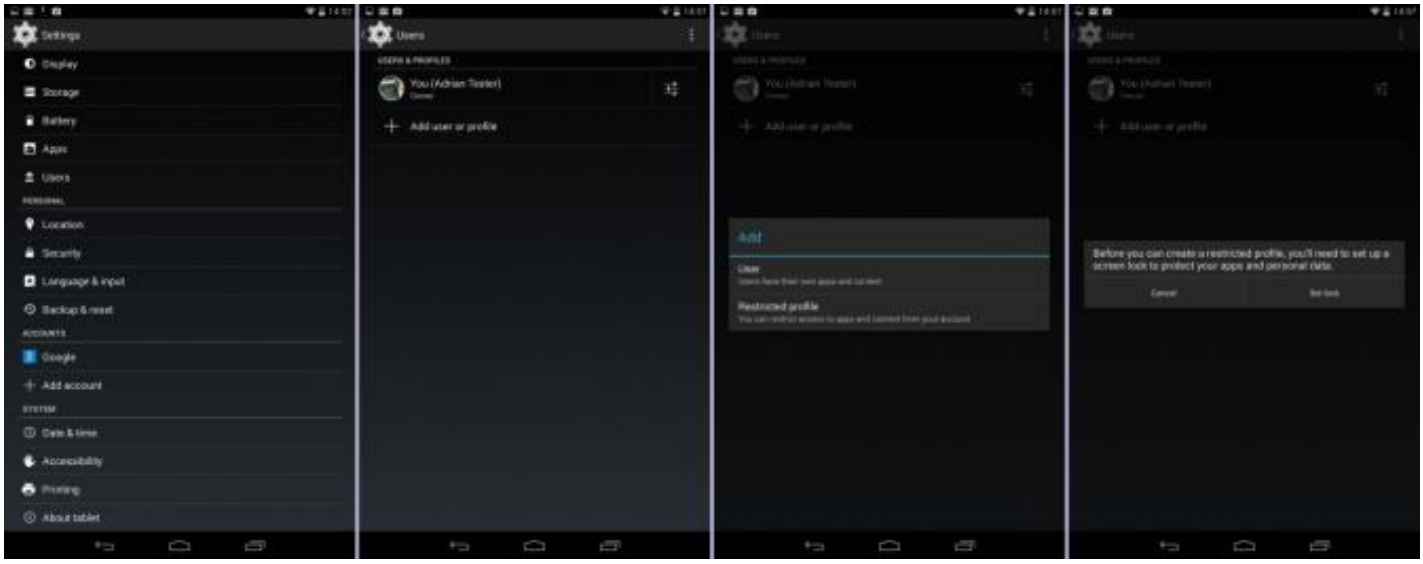
- Accounts
- Find My Friends
- Cellular data use
- Background app refresh
- Volume limit

You can restrict features within Game Center:

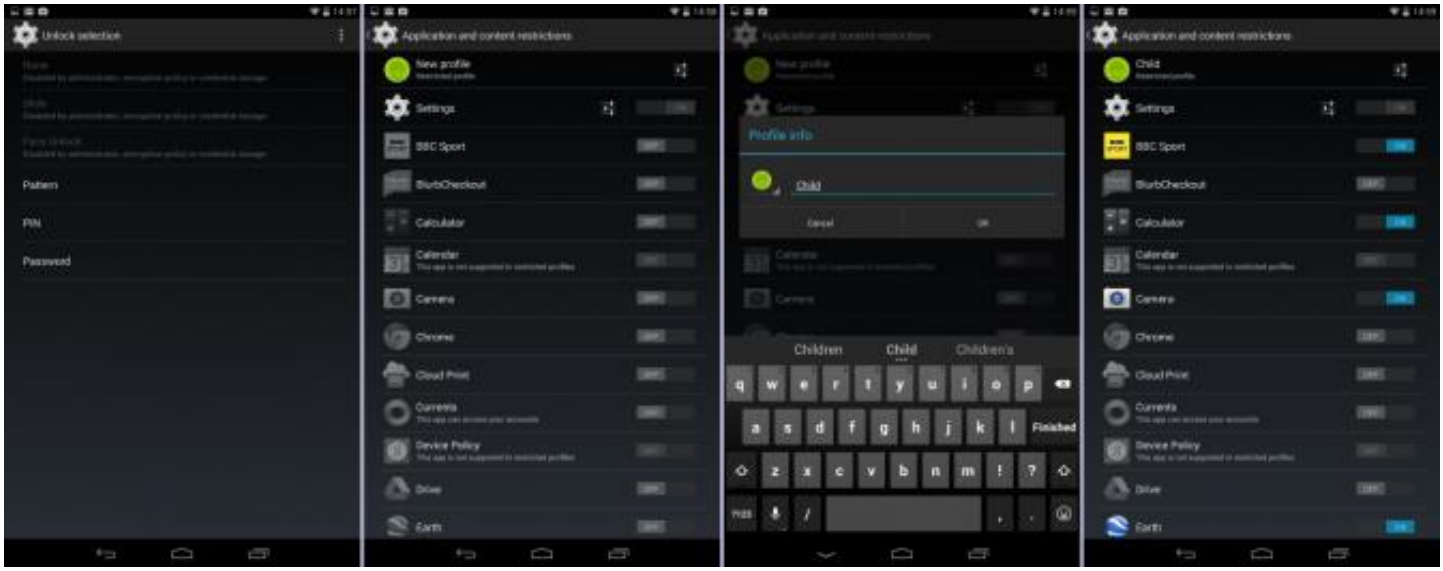
- Multiplayer games
- Adding friends

# Parental Restrictions - Android

If you've got an Android tablet that happens to run Android OS version 4.2 or above, your device should have the power to quickly switch between different user accounts. The main benefit of this is that you can set up one user account for yourself and another for your children to use. With the release of Android 4.3, you can now restrict individual user accounts and block access to apps, games and features which might be inappropriate for your children. Follow the steps below to find out how to create a second user account and exercise parental control over how the account works.



1. Open your **apps list** and tap on the **Settings** icon.
2. Scroll down the settings page until you find **Users**, then press on it.
3. Choose **Add user or profile**. As we're setting this up as a child's account, touch **restricted profile**.
4. At this stage you may be asked to set up a PIN or passcode for your user account. This will only appear if you haven't already secured your profile, and is necessary in order to stop your children bypassing parental controls by simply logging into the phone as you.




1. To add a name to the new account, tap on the **Settings** icon to the right of the new profile and type in a name of your choice.
2. You are now presented with a list of all the apps currently installed on your tablet. Simply scroll down this list, pressing the **on/off switch** to the right of the app name to allow or deny access to that particular app or game. When set to **on**, the app is **allowed**.

# Parental Restrictions - Blackberry Devices

Controls help you have more control over how the features of your child's BlackBerry® smartphone are used – you can block content, turn features on or off and decide what types of communication are available. A password is required to prevent children and other people from changing the settings.

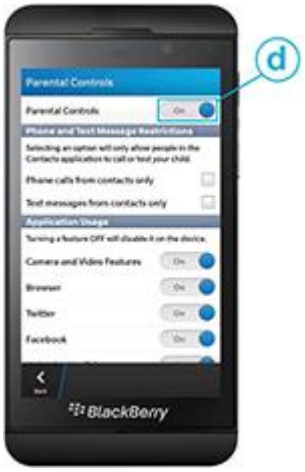
**Step 1 - Turn on Parental Controls**

a. On the home screen or in a folder, click the 'Settings' <Gear> icon.


b. Click 'Security and Privacy'.

c. Click ‘Parental Controls’.


d. Select ‘On’ to turn on Parental Controls.




**Step 2 - Set your Parental Controls password**


Once you have turned on the Parental Controls feature, you will be asked to enter a password. To prevent children or other parties from changing the settings, your password will be required each time you access the Parental Controls menu.

**Step 3 - Select Parental Controls options**

You can select one or more of the following options to allow or limit the use of the Parental Controls feature. Your options will be saved automatically.


**For example:**

- To allow phone calls and text messages from contacts only, select the Phone Calls and Text Messages checkboxes.
- To allow photos and videos to be taken, select the Camera and Video Features checkbox.
- To allow internet access, select the Browser checkbox.
- To allow access to Twitter and Facebook, select the Twitter and Facebook checkboxes.
- To allow the uploading of files to YouTube, select the Upload to YouTube checkbox (NB: This restriction does not limit access to the YouTube website – it only limits the ability to upload videos to the site).
- To allow email accounts to be added and edited, select the Email Account Setup checkbox.
- To allow the use of location services, like GPS, select the Location Information checkbox.
- To allow content to be purchased, select the Purchase Content checkbox. Please note, you can 'allow' or 'not allow' purchases in the BlackBerry® World™ app store as well as in-app purchases for those apps that use the BlackBerry® World™ payment system.
- To allow the installation and removal of third party applications, select the Install Application and Remove Application checkboxes.
- To allow access to BlackBerry® World™ (the app store), select the BlackBerry® World™ checkbox. You can also set Content Restrictions within BlackBerry® World™ at this point.

**Step 4 - Change your Parental Control settings**


If you decide to change the settings at any time (for example, if you decide your child may have access to Facebook on their smartphone once they reach the age of 13), simply follow the instructions below.

1. a. On the home screen or in a folder, click the 'Settings' icon.
2. b. Click 'Security and Privacy', then 'Parental Controls'.
3. c. Enter your password.
4. d. Make changes to your options (these will be saved automatically).

# Useful Websites for Parents

https://www.ceop.police.uk/ceop-reporting/


*If you are concerned about something that may have happened while online, you can take control.* ***If you are in immediate danger or want urgent help call 999 or contact your local police****. Otherwise there are a number of ways to receive help and advice as well as the option to report any instance of sexual contact or harmful material to the at the Child Exploitation and Online Protection Centre. You are doing the right thing and by taking this action you may not only help yourself but also help make other people safer as well.*

www.thinkuknow.co.uk/parents

***Think U Know*** *has a section with advice for parents which is particularly useful for explaining terminology. Register to receive the 'Purely for Parents' monthly email.*

www.childnet-int.org/kia/parents

***Know IT All for Parents*** *is a useful CD which parents can use with their children to make sure that they get the most out of the internet. There is some sample content available on this site. Clicking on home will take you to the* ***Childnet International*** *site.*

www.dcsf.gov.uk/byronreview

*Read* ***Tanya Byron****'s independent review looking at the risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games.*

www.dcsf.gov.uk/ukccis/

*The* ***UK Council for Child Internet Safety (UKCCIS)*** *brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Dr Tanya Byron's report.*

www.getsafeonline.org

***Get Safe Online*** *provides information and advice on using the internet safely at home.*

www.ofcom.org.uk

*Ofcom have great advice for setting parental controls on mobile phones and digital television boxes.*

www.bbc.co.uk/panorama

*Watch* ***Panorama****'s investigation into how paedophiles are using the internet, and social networking sites in particular, as a means of grooming unsuspecting youngsters for sex.* ***'One Click From Danger'.***

# Sites for using with children

www.bbc.co.uk/onlinesafety/
***BBC Online Safety*** *help you use the internet in a safe way. It links to sites that are kept up to date with useful information, along with explanations and helpful hints for you and your family to get the most out of the internet.*

www.kidsmart.org.uk
***Kidsmart*** *has advice for children under/over 11 as well as games. The SMART rules are useful to help young people remember how to stay safe.*

.

---

**Safe searching – information, images and videos**
These are sites which are 'safe' to use when searching.

www.google.co.uk/intl/en/landing/familysafety
***Google SafeSearch*** *When you're searching on Google, you may prefer to keep adult content out of your search results. SafeSearch screens sites that contain sexually explicit content and removes them from your search results. While no filter is 100% accurate, SafeSearch helps you avoid content you may prefer not to see or would rather your children did not stumble across. You can modify your computer's SafeSearch settings by clicking on the Preferences link to the right of the Google search box.*

www.pics4learning.com
*Photographs on a safe site from the US.*

www.arkive.org
*Images and videos of life on Earth.*

http://office.microsoft.com/en-gb/images/?CTT=97
*Microsoft clip art and other images.*

# Acceptable Internet Use at Home

I want to use our computer and the Internet. I agree to follow these rules, and my parents agree to help me follow these rules:

- ✓ I will not give my name, address, telephone numbers, school name or my parents' names, address, or telephone numbers to anyone I meet on the computer. I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.

- ✓ I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they are really grown-ups. I will tell my parents about people I meet online. I will also tell my parents before I answer any emails I get from or send emails to new people I meet online. I will not open any email attachments without asking my parents' permission first.

- ✓If someone asks me to do something I am not supposed to do online I will tell my parents.

- ✓ I will not call anyone I meet online, send them anything, or meet them in person, unless my parents say it's ok.

- ✓ I will not buy or order anything online without asking my parents, or give out any credit card information.

- ✓ I won't say any bad things about people online, be mean to anyone, or use bad language online. I will not get into arguments or fights online. If someone tries to start an argument or says something nasty to me, I won't answer him or her and will tell my parents.

- ✓If I see something I do not like or makes me feel uncomfortable or worried, I will tell my parents.

- ✓ I will not use something I found online and pretend it's mine.

- ✓ I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something. I won't keep secrets from my parents about what I do or see on the computer – even if I'm worried about getting in trouble.

# The Royal Alexandra and Albert School

## ICT Acceptable Use Policy

It is appropriate for people to be allowed freedom in using ICT. With freedom comes responsibility. RAAS cannot control what people, all over the world, make available on the Internet. We endeavour to filter these sites however a small proportion of the material which it is possible to access is not acceptable in school.

We expect **ALL** ICT users using our network to take responsibility in the following ways:

**Take Ownership**
Not to access or even try to access any material which is:
• Violent or that which glorifies violence
• Criminal, terrorist or glorified criminal activity (including drug abuse)
• Racist or designed to incite racial hatred
• Designed to incite religious hatred
• Of extreme political opinion which is intended to incite radical behaviour
• Pornographic or with otherwise unsuitable sexual content
• Crude, profane or with otherwise unsuitable language
• Blasphemous or mocking of religious and moral beliefs and values
• In breach of the law, including copyright law, data protection, and computer misuse

**Respect ourselves, others and the environment**
• The property of other users of ICT systems and which they do not have explicit permission to use
• Not to attempt to install unauthorised and unlicensed software
• Not to use other people's user ID or password, even with their permission
• Not to interfere with or cause malicious damage to the ICT resources and facilities
• To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number, on social networking sites or e-mails to strangers

**Be Courageous and honest**
• To report any breach (deliberate or accidental) of this policy to the Head of IT Services immediately

**Contribute to our community**
• Not to search for, or use websites that bypass the school's Internet filtering
• Not to access personal social networking accounts during normal working hours, lessons or during prep time.
• Not to download or even try to download any software without the explicit permission of a member of the ICT systems support department

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Any use of the ICT may be monitored and recorded, including the contents of e-mail messages, by our security systems to ensure that this policy is followed. The RAAS reserves the right to access all material stored on its ICT system, including that held in personal areas of staff and pupil accounts, including email mailboxes, for purposes of ensuring DCFS, LEA and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who

is found not to be acting responsibly in accordance to school policies (including the schools E-Safety Policy) will be disciplined. Irresponsible users will be denied access to the ICT facilities. RAAS will act strongly against anyone whose use of ICT risks bringing the school into disrepute or risk the proper work of other users. Persistent offenders will be denied access to the ICT facilities – on a permanent basis

# Bypassing Security Filters using a VPN.

We have had the issue until recently in school of students trying to bypass our filters using a Virtual Private Network (VPN). In very simple terms, a VPN connects your PC, smartphone, or tablet to another computer (called a server) somewhere on the internet, and allows you to browse the internet using that computer's internet connection. So if that server is in a different country, it will appear as if you are coming from that country, and you can potentially access things that you couldn't normally. It also can allow you to be anomalous online and to bypass local filters.

In school we now have a filter that is continually updating with VPN Details and blocking them. This has been very successful in combating this issue. At home you need to be aware as children can use these apps on their phones to bypass your home broadband security settings. For example on Sky broadband you can setup Sky Shield to not allow content above a certain age limit. With the VPN turned on this can be bypassed.

The best way to combat this is a mixture of setting parental restrictions on the devices and periodically checking the device for new apps that have been installed.