E-Safety Information for Parents
**Statement of Intent**

In our school, our Christian vision shapes all we do. All members of the school community are committed to upholding the St Michael’s Church of England Christian values:

- to show love, care and kindness to all in our community
- to value what we have and to share with others
- to enable everyone to achieve their full potential

The Internet is a wonderful and diverse place, filled with incredible information resources. However, for many parents and carers, 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 should not 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 guide 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.

This guide includes information and guidance about:

- Top tips for parents
- Social networking and Instant Messenger
- Acronyms and abbreviations
- Online gaming and games consoles
- Grooming
- Cyber bullying
- Computer and online security
- Identify theft
- Mobile phones
- Useful websites
- Acceptable Internet use at home

Updated December 2019
Top Tips for Parents

1. Set up an account for each user on your PC at home and only give yourself administrative 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 on for 5 minutes you will have to enter your password to access your computer. You can do this in the ‘Control Panel’.

3. Encourage your family of use technology in a public part of the house, and not in the bedroom, where it is easier to monitor what your child is doing. This applies not just to PCs but also to laptops, tablets 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 One you can do so by going to ‘Settings, Parental controls’ or use the online account to set up parental controls. There is also the option a 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 favourite 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, SnapChat, Instagram and Twitter. 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: WhatsApp, SnapChat, WeChat, KiK and even Facebook has its own IM service.

Simple Social Networking and Instant Messenger Rules
Pay attention to age restrictions see image below for age restrictions:
Social networking sites, such as Facebook and Instagram, 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 o 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.

For more information visit:
www.thinkuknow.co.uk

Facebook Privacy information can be found here:
https://en-gb.facebook.com/full_data_use_policy

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>Anytime, anywhere, anyplace</td>
</tr>
<tr>
<td>AAM</td>
<td>As a matter of fact</td>
</tr>
<tr>
<td>AB</td>
<td>Ah bless</td>
</tr>
<tr>
<td>ADctd2uv</td>
<td>Addicted to love</td>
</tr>
<tr>
<td>AFAIK</td>
<td>As far as I know</td>
</tr>
<tr>
<td>AFK</td>
<td>Away from keyboard</td>
</tr>
<tr>
<td>AKA</td>
<td>Also known as</td>
</tr>
<tr>
<td>ALLWansU</td>
<td>All I want is you</td>
</tr>
<tr>
<td>AML</td>
<td>All my love</td>
</tr>
<tr>
<td>ASAP</td>
<td>As soon as possible</td>
</tr>
<tr>
<td>ASL?</td>
<td>Age, sex, location?</td>
</tr>
<tr>
<td>ATK</td>
<td>At the keyboard</td>
</tr>
<tr>
<td>ATM</td>
<td>At the moment</td>
</tr>
<tr>
<td>ATW</td>
<td>At the weekend</td>
</tr>
<tr>
<td>AWHFY</td>
<td>Are we having fun yet</td>
</tr>
<tr>
<td>B4</td>
<td>Before</td>
</tr>
<tr>
<td>B4N</td>
<td>Bye for now</td>
</tr>
<tr>
<td>BAK</td>
<td>Back at keyboard</td>
</tr>
<tr>
<td>BBL</td>
<td>Be back later</td>
</tr>
<tr>
<td>BBS</td>
<td>Be back soon</td>
</tr>
<tr>
<td>BBSD</td>
<td>Be back soon darling</td>
</tr>
<tr>
<td>BCNU</td>
<td>Be seein' you</td>
</tr>
<tr>
<td>BF</td>
<td>Boyfriend</td>
</tr>
<tr>
<td>BFN/B4N</td>
<td>Bye for now</td>
</tr>
<tr>
<td>BGWM</td>
<td>Be gentle with me</td>
</tr>
<tr>
<td>BRB</td>
<td>Be right back</td>
</tr>
<tr>
<td>BRT</td>
<td>Be right there</td>
</tr>
<tr>
<td>BTW</td>
<td>By the way</td>
</tr>
<tr>
<td>CM</td>
<td>Call me</td>
</tr>
<tr>
<td>CU</td>
<td>See You</td>
</tr>
<tr>
<td>CUIMD</td>
<td>See you in my dreams</td>
</tr>
<tr>
<td>CUL</td>
<td>See you later</td>
</tr>
<tr>
<td>CUL8R</td>
<td>See you later</td>
</tr>
<tr>
<td>CYA</td>
<td>See you</td>
</tr>
<tr>
<td>DK</td>
<td>Don’t know</td>
</tr>
<tr>
<td>DUR?</td>
<td>Do you remember</td>
</tr>
<tr>
<td>E2EG</td>
<td>Ear to ear grin</td>
</tr>
<tr>
<td>EOD</td>
<td>End of discussion</td>
</tr>
<tr>
<td>F2F</td>
<td>Face to face</td>
</tr>
<tr>
<td>F2T</td>
<td>Free to talk</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently asked questions</td>
</tr>
<tr>
<td>FC</td>
<td>Fingers crossed</td>
</tr>
<tr>
<td>FITB</td>
<td>Fill in the blank</td>
</tr>
<tr>
<td>JFK</td>
<td>Just for kicks</td>
</tr>
<tr>
<td>KC</td>
<td>Keep cool</td>
</tr>
<tr>
<td>KHUF</td>
<td>Know how you feel</td>
</tr>
<tr>
<td>KISS</td>
<td>Keep it simple, stupid</td>
</tr>
<tr>
<td>KIT</td>
<td>Keep in touch</td>
</tr>
<tr>
<td>KOTC</td>
<td>Kiss on the cheek</td>
</tr>
<tr>
<td>KOTL</td>
<td>Kiss on the lips</td>
</tr>
<tr>
<td>L8</td>
<td>Late</td>
</tr>
<tr>
<td>L8r</td>
<td>Later</td>
</tr>
<tr>
<td>LDR</td>
<td>Long distance relationship</td>
</tr>
<tr>
<td>LMAO</td>
<td>Laugh my ass off</td>
</tr>
<tr>
<td>LOL</td>
<td>Laugh out loud</td>
</tr>
<tr>
<td>LTNC</td>
<td>Long time no see</td>
</tr>
<tr>
<td>M8</td>
<td>Mate</td>
</tr>
<tr>
<td>MOB</td>
<td>Mobile</td>
</tr>
<tr>
<td>MTE</td>
<td>My thoughts exactly</td>
</tr>
<tr>
<td>MYOB</td>
<td>Mind your own business</td>
</tr>
<tr>
<td>NA</td>
<td>No access</td>
</tr>
<tr>
<td>NC</td>
<td>No comment</td>
</tr>
<tr>
<td>NE</td>
<td>Any</td>
</tr>
<tr>
<td>NEI</td>
<td>Anyone</td>
</tr>
<tr>
<td>NOI</td>
<td>No-one</td>
</tr>
<tr>
<td>NRN</td>
<td>No reply necessary</td>
</tr>
<tr>
<td>NWO</td>
<td>No way out</td>
</tr>
<tr>
<td>O4U</td>
<td>Only for you</td>
</tr>
<tr>
<td>OIC</td>
<td>Oh I see</td>
</tr>
<tr>
<td>OTOH</td>
<td>On the other hand</td>
</tr>
<tr>
<td>PCM</td>
<td>Please call me</td>
</tr>
<tr>
<td>PITA</td>
<td>Pain in the ass</td>
</tr>
<tr>
<td>PPL</td>
<td>People</td>
</tr>
<tr>
<td>PRT</td>
<td>Party</td>
</tr>
<tr>
<td>PRW</td>
<td>Parents Are Watching</td>
</tr>
<tr>
<td>QT</td>
<td>Cutie</td>
</tr>
<tr>
<td>R</td>
<td>Are</td>
</tr>
<tr>
<td>RMB</td>
<td>Ring my Bell</td>
</tr>
<tr>
<td>ROTFLMAO</td>
<td>Rolling On The Floor Laughing</td>
</tr>
<tr>
<td>RU?</td>
<td>Are you?</td>
</tr>
<tr>
<td>RUOK?</td>
<td>Are you ok?</td>
</tr>
<tr>
<td>SC</td>
<td>Stay cool</td>
</tr>
<tr>
<td>SETE</td>
<td>Smiling ear to ear</td>
</tr>
<tr>
<td>SK8</td>
<td>Skate</td>
</tr>
<tr>
<td>SMEI</td>
<td>Someone</td>
</tr>
</tbody>
</table>
FWIW For what it's worth
F? Friends
EOL End of lecture
FYA For your amusement
FYEO For your eyes only
FYI For your information
G9 Genius
GAL Get a life
GG Good game
GMTA Great minds think alike
GF Girlfriend
GSOH Good salary, own home, 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
IMII 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
SO Significant other
SQL 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
URTI 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 PlayStatiton, 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. See page 6 for more information regarding this.

For more information about online gaming visit: www.askaboutames.com
Games Consoles
On the PlayStation 4™ parents and guardians can set security levels to restrict access to games depending on age ratings. DVD and Blu-ray movies can also be blocked completely.

How to set parental controls and spending limits on PS4

How to set monthly spending limits
1. Go to [Settings] > [Parental Controls/Family Management] > [Family Management].
2. Select the user you want to set a spending limit for, then select [Applications/Devices/Network Features] under the Parental Controls section.
3. Select 'Monthly Spending Limit' and press X

How to restrict access to Network Features
1. Go to [Settings] > [Parental Controls/Family Management] > [Family Management]. You may need to enter your account password.
2. Select the user you want to set restrictions for, then select [Applications/Devices/Network Features] under the Parental Controls section.
3. Under 'Network Features' you can choose whether to allow a child family member to communicate with other players on PSN or view content created by other players.

How to set age rating levels for games, Blu-ray Discs and DVD videos
Follow the steps below to set age rating levels for games. Before you do this, make sure you know the appropriate parental control level for your child.
1. Go to [Settings] > [Parental Controls/Family Management] > [Family Management]. You may need to enter your account password.
2. Select the user you want to set the age level for, then select [Applications/Devices/Network Features] and select the content you would like to restrict.

How to prevent children changing parental controls
The steps below can help you keep your parental control settings secure, and prevent children from attempting to override or change the settings without the family manager's permission.
1. Disable new user creation and guest login
2. Set a login passcode
3. Set a system restriction passcode

For more information visit https://www.playstation.com/en-gb/get-help/help-library/my-account/parental-controls/ps4-parental-controls/

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 and limit purchases made through the console.

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 x to select.
2. Scroll down to Parental Controls and press x.
3. Enter your PIN Number then press x (the default PIN Number if you have not previously changed it is 0000).
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.

**Time Limits**

**How to set time limits on the Xbox One**

Time limits can only be set through your Microsoft account in your browser. You can make them apply to the console as well as to the PC.

1. Sign in to your Microsoft account.
2. On your family page, scroll to your kid's name and select Screen Time. (If you don’t see your kid's name, use "Add a family member" to add their account to your family group or create a new account for them if needed.)
3. To set one limit that applies to both the Xbox and the PC, turn on "Use one screen time schedule."
4. To manage time limits separately, scroll down and turn on screen time for Windows devices or Xbox, whichever you want to set first.
5. Click "Set a time limit." Then choose a start time and an end time for each day of the week.
6. You can program the Xbox to send a notification to your kids when their screen time is ending.
7. To do this, press the Xbox button on the controller.
8. Select System > Settings > Preferences > Notifications > Xbox Notifications > System and turn on "System notifications." Your kid will see the clock count down when time is ending.

**Chat**

**How to turn off chat on the Xbox One using the console**

These settings are found in the privacy and online safety section and also turn off other social features.

1. Sign in to your Xbox.
2. Press the Xbox button to open the guide. Then go to System > Settings > Account.
3. Select Family settings > Manage family members.
4. Choose a family member, then select Privacy & online safety > Xbox Live privacy > View details and customize > Communication & multiplayer.
5. Select the setting "You can play with people outside of Xbox Live" and click "block" to turn it off. (This prevents all cross-network play -- for example, between your kid on her Xbox and her friends on their PlayStations or Nintendos.)
6. Alternatively, if you’re OK with your kid playing cross-network but not OK with them talking and texting with strangers, allow cross-network play but restrict chatting to specific people. Select "You can communicate outside of Xbox Live with voice & text" and designate a player or players with whom your kid can talk within a specific game.

**Mature Content**

**How to limit mature content on the Xbox One using the console**

You can limit access to games as well as websites on the Xbox.

1. Sign in to your Xbox.
2. Press the Xbox button to open the guide. Then go to System > Settings > Account > Family.
3. Select "Manage family members" and then find your kid’s name and select "Access to content," then select the age limit you feel is appropriate for your child. Microsoft automatically sets default age restrictions for kids, but you can customize them.
4. Go back to the Family page and select "Web filtering." Select the drop-down menu to view the available options.
5. When your kid requests to use a blocked app or game, you can approve it and add it to the Always allowed list, which is under Content restrictions. You can also add websites to Always allowed. You can respond to their requests from your email, from your family profile, or in person, of course.

Purchasing

How to block purchases on the Xbox One using the console

This lets you manage your families’ purchases by requiring your approval.

1. Sign in to your Xbox.
2. Press the Xbox button to open the guide. Then go to System > Settings > Account > Family settings > Manage family members.
3. Select your kid’s account.
5. Select the Ask a Parent box.

For more information, visit https://www.commonsensemedia.org/blog/parental-controls-xbox-one

The Nintendo Switch 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.

When you first set up your Switch, you can enable Parental Controls from the set-up screen. You can also enable them at any time from System Settings on the Switch console.

1. Launch System Settings from the Home screen on your Nintendo Switch.
2. Scroll down and select Parental Controls.
3. Select Parental Controls Settings on the right side of the screen.
4. Select Use this console.
5. Select Restriction Level.
6. Select Teen, Pre-Teen, or Child to create a pre-made setting.
7. Select Custom Settings to manually configure your parental control settings.

For more information, visit https://www.nintendo.co.uk/Support/Nintendo-Switch/Parents/Parental-Controls/Setting-Parental-Controls/Setting-Parental-Controls-1198700.html

For more information about games consoles visit: https://www.askaboutgames.com/
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.

For more information visit:
https://www.thinkuknow.co.uk/parents/articles/Online-grooming/

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.

For more information visit:
https://www.bullying.co.uk/cyberbullying/
Computer And Online Security

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:  
https://www.getsafeonline.org/

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 response 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:  
https://ico.org.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.

www.childnet.com

<table>
<thead>
<tr>
<th>Questions to Ask</th>
<th>Background</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safety Advice</strong></td>
<td>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.</td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Internet Access</strong></td>
<td>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.</td>
</tr>
<tr>
<td>• Does this phone have Internet access?</td>
<td></td>
</tr>
<tr>
<td>• Is there a filter to help block Internet content that is particularly harmful for children?</td>
<td></td>
</tr>
<tr>
<td>• Is the filter switched on? If no, can you switch it on please?</td>
<td></td>
</tr>
<tr>
<td><strong>Registering the Phone</strong></td>
<td>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.</td>
</tr>
<tr>
<td>• Is the phone registered for a child or for an adult user?</td>
<td></td>
</tr>
<tr>
<td><strong>Bluetooth-enabled Phones</strong></td>
<td>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. 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.</td>
</tr>
<tr>
<td>• Is this phone ‘Bluetooth-enabled’?</td>
<td></td>
</tr>
<tr>
<td>• How can I turn this off, or set it so the phone is not visible to others?</td>
<td></td>
</tr>
<tr>
<td><strong>Premium Rate Calls and Texts</strong></td>
<td>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</td>
</tr>
<tr>
<td>Questions to Ask</td>
<td>Background</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• If you cannot bar these numbers, what services do you provide to protect the</td>
<td>text from. This will end the service and your payments to it.</td>
</tr>
<tr>
<td>user here?</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chatrooms and Gaming</td>
<td>Chatrooms or games (where you can chat to other users)</td>
</tr>
<tr>
<td>• Can this phone access chatrooms or games where users can chat to each other?</td>
<td>what are provided by your mobile operator or its partners and which do not have an 18+ age-restriction</td>
</tr>
<tr>
<td>• Are these chatrooms or games moderated?</td>
<td>must be moderated.</td>
</tr>
<tr>
<td>• How are the chatrooms or games moderated?</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Nuisance/Malicious Calls</td>
<td>Your mobile operator should have systems and procedures in place to help you deal with nuisance and</td>
</tr>
<tr>
<td>• What number can I call to report receiving unwanted or abusive calls or</td>
<td>malicious phone calls.</td>
</tr>
<tr>
<td>messages?</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reporting Abuse</td>
<td>It is important to let your mobile operator know if their system is failing, both in order to protect</td>
</tr>
<tr>
<td>• Where do I report abuse of service? If for example I receive unwanted adult</td>
<td>yourself and others using the same service.</td>
</tr>
<tr>
<td>(18+) material on my phone while the filter is switched on, who should I report</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>this to?</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SPAM</td>
<td>Your mobile operator will take action against SPAM, whether it is text, picture or email. Find out</td>
</tr>
<tr>
<td>• What action is your Mobile Operator taking to prevent SPAM?</td>
<td>what action your mobile operator is taking and report any SPAM received on your phone to them.</td>
</tr>
</tbody>
</table>

Mobile phone provider advice for parents:
https://www.o2.co.uk/help/nspcc
https://www.vodafone.co.uk/mobile/digital-parenting/parental-controls
https://ee.co.uk/our-company/corporate-responsibility/keeping-children-safe-online
Useful Websites

Sites For Parents
https://www.ceop.police.uk/safety-centre/
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 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.

https://www.thinkuknow.co.uk/parents/
Think U Know has a section with advice for parents which is particularly useful for explaining terminology.

https://www.childnet.com/
Childnet International provide information for parents/carers, children and education professionals to help keep children safe in the digital age.

To read Dr Tanya Bryon’s report on keeping children safe in a digital world.

https://www.gov.uk/government/organisations/uk-council-for-internet-safety
The UK Council for Internet Safety (UKCIS) 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.

https://www.getsafeonline.org/
Get Safe Online provides information and advice on using the Internet safely at home.

www.ofcom.org.uk
Ofcom has great advice for setting parental controls on mobile phones and digital television boxes.

http://www.bbc.co.uk/webwise/topics/safety-and-privacy/
The BBC helps you to 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

https://www.safesearchkids.com/
Google SafeSearch: when you’re searching on Google, you may prefer to keep adult content out of your search results. Safe Search screens sites that contain sexually explicit content and removes them from your search results. While no filter is 100% accurate, Safe Search 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 Safe Search settings by clicking on the preferences link to the right of the Google search box.
http://www.pics4learning.com/
Photographs on a safe site from the US

http://www.dorlingkindersley-uk.co.uk/static/cs/uk/11/clipart/home.html
Clip art from Dorling Kindersley.

http://clipart-library.com/microsoft-cliparts.html
Microsoft clip art and other images.

https://www.commonsensemedia.org/

Other Useful Links
Have a conversation about online safety
https://www.childnet.com/parents-and-carers/have-a-conversation
https://www.Internetmatters.org/

Setting app privacy settings
https://www.Internetmatters.org/
E-safety advice for parents
https://www.Internetmatters.org/

Sexting
https://www.Internetmatters.org/
Acceptable Internet Use at Home

I want to use our computer and 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 of 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 receive from or send emails to new people I meet online.

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 is ok.

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

I will not 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 will not 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 is mine.

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

I promise to follow these rules (you sign here!)

I promise to help my child follow these rules (your parent signs here!)