

Online Safety Introduction

Technology is rapidly developing and our children have access to an increasingly wide range of devices and media. These communication methods can be incredibly useful and powerful but they can also make students vulnerable both from their own actions and from other people.

As online technology, software and apps develop in it is hard to stay up to date with how our young people are interacting with the world and what we should do to keep them safe.

The constantly changing and evolving world of online and electronic communication is very exciting and offers young people incredible opportunities to engage and interact with their friends and from people from all over the world in very positive ways. We need to help them explore and learn about these as safely as possible. The biggest four tips for keeping safe would be:



- Check your privacy settings – most websites, Apps and social networks allow different levels of settings, you should always make them as private as possible and keep checking them regularly as sometimes updates make your account more public.
- Don't share personal info – this is the big obvious stuff like posting your address and birthday to smaller staff like making sure that your photos aren't GPS stamped, or that you take photos in your school uniform, outside your house, in front of your parents car with its registration showing.
- Don't arrange to physical meet someone you have met on the internet unless your parents know and you meet in a public place.
- Don't post anything – a picture, video or message that you don't want the whole world to see. Even if you only send it to one person as soon as it has left your device you lose control.



Our own website has some useful tips on online safety including a link to CEOP (child exploitation and online protection) and a link to [The Sharp System](#) that students or parents can use anonymously to report bullying or abuse both at the bottom of the home page. There is also a request for support with [online safety button](#) for parents and carers in the online safety tab.

Parenting in the Digital Age – free online training for parents

Our school is part of Parent Zone's Digital Schools Membership programme, recognising our commitment to keeping our pupils safe online, and making sure we work with you and all of the school community to achieve this.

Digital Schools membership includes access to Parent Zone's online digital parenting course, Parenting in the Digital Age. This short course gives you straightforward information and advice on how to manage and feel confident about your child's online world.

For your free access to the programme, go to www.parentzone.org.uk/parentcourse.

- Click on the pink 'Add to cart' button to start your registration.
- On the next page click checkout. You'll then be asked to enter your email address.
- On the next page, you will need to enter the coupon code **DSP16** to ensure you have free access to the programme. The code gives you 100% discount on the price of the training.

Once you've completed the short registration you'll receive two emails - one confirming your order and one with log in instructions. After clicking the link in the email press the log-in button and you should be asked to set a password, after which you will be directed to the Parent Resources page where you can start the course.

Once you have logged in the Parenting in the Digital Age course page will always be accessible at this link: <https://parentzone.org.uk/advice/parenting-digital-age-online-course-parents>.

Another benefit of our Digital Schools membership is access to an email help service for parents, so if you have any questions about the course or any aspect of your family's online life, you can email ds-help@parentzone.org.uk for free, confidential advice.

Parental Controls

The NSPCC is leading a campaign that looks at how innocent search terms can lead to adult responses for children and has some good ideas about how to install parental controls on a range of devices here:

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/parental-controls/>

Current Apps

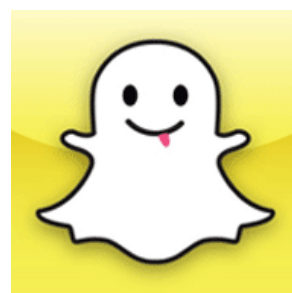


ooVoo is a free App that works on any device, for example smart phones, tablets or laptops. It enables up to 12 people to video and text message at any one time. It is a great tool to stay in touch with friends, collaborate on work or for joint revision sessions. There are risks however – because it is a social network students could be at risk of cyber bullying or get involved in behaviour that they would steer clear of in face:face conversations. When ooVoo is installed for the first time it defaults to public – open to the world and even when privacy is set higher strangers can still see profile pictures etc. The free version of ooVoo generates income through advertising and some of the adverts are for adult websites.

More information about helping young people stay safe on ooVoo can be found here:

<https://www.net-aware.org.uk/networks/ooVoo/>

Snapchat is a photo sharing app for all devices. It allows people to take and edit photos and then send them to their friends. In theory the photos have a very limited life on the receiving friends' device – which can encourage people to send pictures that they don't want staying around. However there are lots of ways that the photos can be kept. The simplest and most used is people just taking a screen shot of the picture message, however there are also apps available that save all incoming messages by default and do not send notification to the original sender.



It is really important that young people think about what they send and to whom as once the picture is sent it could quite easily be sent on around the web in a matter of days.

More information about keeping young people safe on Snapchat can be found here:

<https://www.net-aware.org.uk/networks/snapchat/>



Kik is a relatively new alternative to WhatsApp in the UK. Like WhatsApp it offers free picture and text messaging through the internet from mobile phones. However it also works on tablets and laptops as it does not use a mobile number to create your account. When you install WhatsApp it searches through your phonebook and adds anyone else with a WhatsApp account to your contact list. This is helpful and often means that parents and guardians can keep an eye on their child's online activity.

With Kik you create a username like you would for a website – this means you can choose who you send that username too. Some young people then use Kik to communicate without their parents knowing as they are not included in the network.

You may occasionally see “kik me” written on other networks – this is to encourage the conversation to move to this newer platform – perhaps aware from scrutiny?

Kik has been around in Australia for quite a long time so for more information about keeping young people safe on Kik please follow the link below:

<https://www.common sense media.org/app-reviews/kik-messenger/user-reviews/adult>

Instagram is a photo and video sharing app. It allows users to take, edit and share photos instantly. Originally Instagram was aimed at photographers rather than as a social network and as such it is automatically public when an account is opened. This means that all photos can be seen by anyone in the world. It is really important to make sure privacy settings are updated before photos are uploaded. Like Twitter once your account is live you can choose to follow people and see their uploaded photos. Similarly people can follow you and see your photos. Judging whether these people are genuine is a very difficult task and so it is important to think about what kind of photos you are sharing and who you may be sharing them with.



More information about keeping young people safe on Instagram can be found here:

<https://www.net-aware.org.uk/networks/instagram/>

The following websites are all good sources of reliable information for keeping safe online and are relevant to adults as well as young people.

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

<http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/>

<http://www.saferinternet.org.uk/>

<http://www.bbc.co.uk/webwise/0/21259413>

www.thinkuknow.co.uk

If you are concerned about your child's behaviour online please contact their Student Support Manager so that we can work together to make sure they are safe from harm.

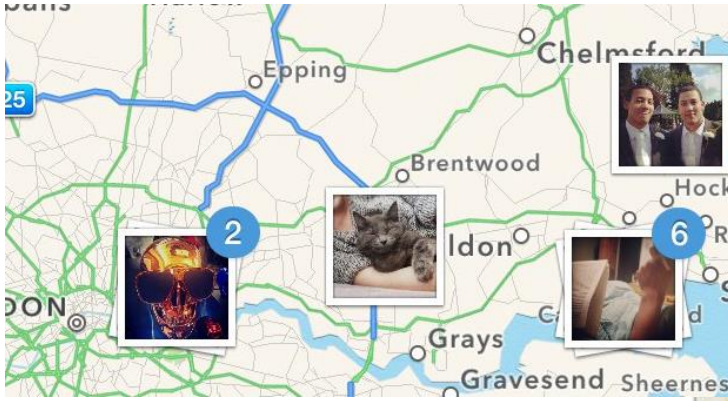
Geo Tagging

As smart phone and tablet technology continues to improve and develop the possibilities and risks for young people also change.

Devices with Global Positioning Satellite (GPS) links or Wifi connections are now able to Geo Tag photos – this means that as well as the photo the device saves the exact location and time the photo was taken. This can be a great way of organising your holiday snaps or remembering an important event however it also exposes students to an increased risk.

When the pictures are shared or posted on social media sites like Facebook or through Apps like Instagram the Geo Tag data can also be accessed in some instances. This means that it is possible to see where a photo was taken. If a young person takes selfies at home it then reveals their home address, or if they take and upload photos at an event again it can reveal their exact location.

On all devices and Apps there are ways of turning off these Geo Tagging or location settings and we would advise that turning them off is the safest default position.



Example of Geo Tagged photos on a map in Instagram – these ones suggest where the user lives as there is a high number of pictures from one location.

A location pin dropped automatically by Facebook on a map where a message or status update is sent from.



map to show

Turning Off Location Settings

Android Devices

To turn off Location Services for your Android device:

1. Tap **Settings > Location**
2. Tap to turn off Location Services (so that it goes grey)

In older Android devices (OS 5.1.1 and earlier), turning off Location Services automatically turns off location access for the Facebook app.


iOS Devices

To turn off Location Services for your iOS device:

1. Tap **Settings > Privacy > Location Services**.
2. Tap near **Location Services**. (so that it goes grey)

Turning Location Services off in Facebook.

To turn on location access for the Facebook app for Android (OS 6.0+):

1. Tap **Settings > Apps >  > App Permissions > Location**
2. Scroll through the list of apps and tap near **Facebook** (so that it goes grey)

3. Restart the Facebook app for Android

To turn off location access for the Facebook app for iOS (version 8.0+):

1. Go to your device's home screen.
2. Tap **Settings > Privacy > Location Services**.
3. Scroll through the list of apps below, tap **Facebook** and select **Never**. If you previously turned on Location History for Facebook, you can select **Never**.
4. Restart the Facebook app for iPhone or iPad.

Turning Off Location in Instagram (iOS)

1. Leave the Instagram app and go to your iPhone's Settings.
2. Tap Privacy > Location Services.
3. Scroll down and tap Instagram.
4. Decide to allow location access Never or While Using the App

It is possible to check and delete existing Geo Tags in Instagram by following the process below:

To see what you're sharing, go to your profile page and click the little gray place marker tab, second from the right. If it's grayed out and you can't click it, you're good to go. If it's clickable, you'll be met with a zoomed-out map of every photo with a geotag.

Then, head into the tab with the map of your photos. Next, you'll want to select "Edit" in the upper right corner, and you'll see your photo counts change from blue to green on the map. Zoom out to select a cluster of photos if you need to, and click on the photo icon.

Here's the confusing part: You'll be met with a grid of your photos from that location and only two buttons, "Select All" and "Deselect All." There's no wording about removing geotags or deleting location data at all. It's not obvious, but if you choose Deselect All > Done, you'll be met with a pop-up message confirming that you want to remove X number of geotags. Click confirm and your historical whereabouts will be wiped from the map.

Sexting: A Parents' Guide

According to the NSPCC, *sexting* is more commonplace than we may think. In 2014/15 over 1,200 ChildLine counselling sessions mentioned 'sexting' in some way, and it seems to be on the increase.

We at St Peter's take online safety very seriously, and we want to take this opportunity to guide you through the ins and outs of sexting; the risks, what you can do to protect your family, and what you can do if something goes wrong.

What is Sexting?

- Sexting is when someone *sends* or *receives* a **sexually explicit** text, image or video.
- Usually via a **mobile phone**, but any device which connects to the internet can be used (like a tablet or a laptop).
- Sometimes referred to as '**cybersex**' or 'sending a **nudie**/nude selfie'
- Sexting is often seen as **flirting** and many young people see it is a part of **normal life**.
- Sometimes, it can be the result of **coercion**, peer pressure or **bullying**.

What Are the Risks?

- Once the message or image has been sent, **control** is lost. The image could easily end up anywhere on the internet which could cause a lot of **distress**.
- Sexting could leave a young person **vulnerable** to blackmail, **bullying**, unwanted attention and emotional **distress**.
- Images are **never** safe – even if using apps which delete it after a few seconds (like **Snapchat**). Someone could easily take a picture of the screen using **another phone** for example...
- It's **illegal** – the police try to avoid criminalising children, but by sending explicit images a young person is still **breaking the law**, even if it of themselves.

Should I Talk to My Child About Sexting?

- **Yes**. It may be **awkward**, but we believe you must have that conversation.

How?

- Let them know that you **understand** their point of view, but that they must think **carefully** about what they are sending and to **whom**. Talk about what they think is and isn't **appropriate**.
- Let them know that if they *ever* have concerns that they can talk to you, or to a member of **staff** at St Peter's.
- Reassure them that you will be **supportive** and **understanding**, and they can come to you if someone asks them to **send** an explicit message, or if they have **seen** or **shared** something which worries them – you just want them to be **safe** and **happy**.
- Ensure they know that saying '**no**' is ok – after all, they are **in charge** of what they share.
- Explain the **risks** – if they wouldn't want the **world** to see it, they shouldn't send it. Images can easily be **copied** and **forwarded**.
- Use some of the **resources** below to help start a conversation.

More Help and Advice

Below are a few other **resources** specifically relating to sexting, some of which may help begin the **conversation** with your child.

www.childline.org.uk/sexting

www.nspcc.org.uk/sexting

www.childnet.com/sexting

And finally...

If you have any **questions** or **concerns**, or your child has been **affected** by sexting, please do not hesitate to get in contact with your child's **Student Support Manager**, and we will do our very best to **help** you.