



Police Scotland

Sanquhar and Wallace Hall

Newsletter

April—2021

Youth Engagement Officer—Sanquhar/Wallace Hall

This is my first Newsletter and hopefully over the course of the year each of the Youth Engagement Officers will compile a termly Newsletter with any issues that may arise. Can I begin by thanking everyone for their efforts during this very challenging COVID -19 pandemic. Hopefully now there is some light at the end of this long journey for us all, it is great to see all pupils back in school safely and receiving their education.

I have been in post as Youth Engagement Officer for 2 years, however I have over 17 years' Police Service, serving in a variety of roles throughout Dumfries and Galloway. I started my service as a Police Cadet, progressing into Response Policing and thereafter Community Policing Unit serving the communities both in Dumfries and Mid and Upper Nithsdale. I also spent some time within the Traffic Department Policing the A74(M) at Lockerbie.

Due to the restrictions placed upon us all during the COVID -19 pandemic, it has been difficult to engage with both pupils and parents. However I hope to be able to be able to re-attend important events within the schools over the next few months. I will be back in school this term to deliver any PSE lessons on various topics like CEOP, Substance Misuse, Anti Social Behaviour and Hate Crime.

Through my Newsletters I would like to keep pupils and parents updated on any issues that are being reported, or any issues or concerns we may have within the Police Service that may have an impact on our young people.

I'm aware that a lot of children during the pandemic were home schooling which involved the use of the internet which can be a great tool for adults and young people alike to learn.

Most young people do use Social Media and the Internet as a platform to communicate with their peers, gaming etc. Connecting and sharing information between peers can bring it's own set of risks on Social Media or the Internet, can we ensure please that we keep our privacy settings turned on, can we ensure that we know exactly who we are communicating with to keep ourselves safe at all times. There have been incidents reported to Police in the last few weeks involving snapchat with inappropriate behaviour and messages contained on these platforms

In the meantime please stay safe and look forward to seeing you all soon. **PC Adair**



Constable Gary Adair



<https://cool2talk.org/>

How should I use privacy settings?
Follow these tips to help your child explore the internet safely. If you have an older child who creates their own accounts, consider these tips when talking to them about how they can use privacy settings.

1. Check the audience
2. Switch off location sharing
3. Check the tagging settings #



Advice For Online Safety

As a parent or carer you play a key role in helping your child to stay safe online.

You don't need to be an expert on the internet to help keep your child stay safe online. There is advice and resources available online to support you as you support your child to use the internet safely, responsibly and positively.

The links below, which are very informative and easy to follow, will open up the opportunity for you to start the discussion about online safety. Thinkuknow is the online safety education programme from the National Crime Agency (NCA) and their website has home activity packs from the ages of 4yrs to 14+yrs to take support from.

<https://www.thinkuknow.co.uk/parents/Support-tools/home-activity-worksheets/>

CEOP, NSPCC and Internet Matters, at the links below, have created a number of fantastic free to use advice hubs to help you learn more to support you and your child or young person with Online issues.

<https://www.ceop.police.uk/safety-centre/>

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

<https://www.internetmatters.org/advice/>

Please take time to enhance your knowledge in terms of the support that is available.



SEXTORTION

A SELF-HELP GUIDE



POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Sextortion refers to a specific type of cyber-enabled crime in which victims are lured into performing sexual acts in front of their webcam.

Unbeknown to victims, their actions are recorded by criminals who then use the video footage in an attempt to blackmail them. Generally criminals request money

and if demands are not met, these offenders threaten to upload the recording(s) to the internet and send to the victims' friends and family.

VICTIM REASSURANCE

- Don't panic
- Police Scotland will take your case seriously
- We will not make judgements on your behaviour
- The matter will be dealt with in absolute confidence

VICTIM ADVICE

- Do NOT delete any correspondence
- Do NOT pay
- Do NOT communicate further with the offenders
- DEACTIVATE your accounts
- REPORT online indecent images to the host website

OBTAIN THE FOLLOWING INFORMATION AND PASS ON TO THE POLICE

1. The Skype name, and more importantly;
2. The Skype I.D.; Be aware that the scammer's Skype name is different to their Skype ID, and it's the ID details we need. To get that, right click on their profile, select "View Profile" and then look for the name shown in blue rather than the one above it in black. It will be next to the word "Skype:" and will have no spaces in it.
3. The Facebook URL;
4. The Western Union or MoneyGram Money Transfer Control Number (MTCN);
5. Any photos that were sent

HOW TO REMOVE INDECENT IMAGES

GOOGLE

You can ask Google to remove a nude or sexually explicit image or video of you that's been shared without your consent. To do this:

1. Click on **Settings** in bottom right-hand corner
2. Select **Search Help**
3. Expand **Troubleshoot & Request Removals** from menu
4. Finally click on **Remove information from Google** and follow the step by step instructions

TWITTER

You do not need an account to remove information about yourself. Fill out a form at the following address:

https://support.twitter.com/forms/private_information

FACEBOOK

To report a photo or video:

1. Click on the photo or video to expand it
2. Click on the ellipsis (•••) or the drop down in the top right
3. Click 'I don't like this photo' or 'report this post'
4. Choose relevant option for example 'I think it shouldn't be on Facebook'

YOUTUBE

How to flag a video:

1. Below the YouTube video player click the **More** button
2. Highlight and click the **Report** button in the drop-down menu
3. Click the reason for flagging that best fits the violation within the video
4. Provide any additional details that may help the review team make their final decision

Produced with kind permission of Hampshire constabulary



AMAZON SCAM

A new and dangerous scam is circulating in various forms, which could prove dangerous if people come into contact with it. Persons in our local communities have reported receiving a number of emails which urge them to take action on their Amazon account. The email even contains an official looking watermark complete with the Amazon logo as well as the official address of the organisation's headquarters. Both emails are illegitimate correspondence and by clicking the link and inputting personal information, this is likely to be intercepted by fraudsters who are looking for personal and sensitive information. The consequences, therefore, could be disastrous with people standing to potentially lose a significant amount of money.

PAYPAL SCAMS

PayPal have a long list of the types of scams that they are aware of.

Here are some helpful tips on how to spot Scam Emails:

The Sender's Address

The "From" line may include an official-looking address that mimics a genuine one.

Generic Greetings

Be wary of impersonal greetings like "Dear User", or your email address. A legitimate PayPal email will always greet you by your first and last name.

Typos/Poor Grammar

Emails sent by popular companies are almost always free of misspellings and grammatical errors.

False Sense of Urgency

Many scam emails tell you that your account will be in jeopardy if something critical is not updated right away.

Links

Check where a link is going before you click on it by hovering over the URL in an email, and comparing it to the URL in the browser. If it looks suspicious, don't click it.

Attachments

A real email from PayPal will never include attachments. You should never open an attachment unless you are 100% sure it's legitimate, because they can contain spyware or viruses.

Tracking number

The email/SMS asks you to provide the tracking number of the dispatched item, before you've received a payment into your PayPal account.

Clicking on links

Never click on a link in an email that requests personal information. Any time you receive an email about your PayPal account, open a new browser, type in www.paypal.co.uk, and login to your account directly.

