Community Council Report

This report covers progress we have made in dealing with your priorities for the Kincardine and Mearns Community Council area for the period October 2024.

The report aims to highlight emerging issues in your area, provide crime prevention advice and guidance to Community Council members and the residents you represent. Our focus is to reduce crime and disorder, help create safer communities and respond effectively to local concerns.

In this report I will focus on Police Station 'areas' as historically these stations would covers the following areas.

Portlethen and surrounding areas including Drumoak and Durris. I will specify this as Portlethen.

Stonehaven Police Station – Stonehaven, Newtonhill and surrounding areas. I will specify this as Stonehaven.

Laurencekirk Police Station – Laurencekirk and surrounding areas including Fettercairn, Edzell woods, Auchenblae and Garvock. I will specify this as Laurencekirk.

The A92 towns (Catterline – St Cyrus) along the coastal Road are covered between Stonehaven and Laurencekirk but I will specify them as Coastal Road.

Community Policing Priorities

Antisocial behaviour, Violence and Disorder:

Area	Youth Disorder	Anti-Social
Portlethen	3	3
Stonehaven	7	23
Laurencekirk	1	1
Coastal Road	2	4

Acquisitive Crime: D – Detected UI-Under Investigation

Area	Thefts	Shopliftings	Theft of motor vehicle	Housebreakings/Attempts
Portlethen	2UI	2UI	0	0
Stonehaven	1D,2UI	1D,3UI	0	2D,1UI
Laurencekirk	1UI	0	0	0
Coastal Road	0	0	0	0

Road Safety & road crime:

Area	Careless Driving	Drink/Drug Driving	Dangerous
Portlethen	3D	0	0
Stonehaven	1D	1D	0
Laurencekirk	1D	0	0
Coastal Road	0	1D	0

Community Engagement & Reassurance:

This month we are bringing it back to internet safety for yourself and your loved ones.

How can I protect my identity and surf the internet safely?

Here are some tips:

- Keep your computer browser and security software up-to-date, use firewall and spam filters
- Block spam emails
- Use Wi-Fi at home but make it secure (if you can get onto the Wi-Fi without security data then so can someone else nearby)
- Be cautious if using public space Wi-Fi and never enter passwords or personal data
- Never click on an e-mail link from an unknown source
- Opening fake emails can infect your computer with a virus, allowing someone to remotely access and control your system and data
- Avoid risky websites, including supposed investment sites
- Always change default passwords as soon as you can with strong passwords with random characters
- Avoid passwords like dates of birth and mother’s maiden name
- Don't respond to unsolicited e-mails or telephone calls asking for you to provide some of your personal information for example, your name, date of birth, national insurance number
- Banks and financial institutions do not send emails asking you to confirm your bank details by clicking on a link. Do not trust such emails, no matter how real they look. You can always call your bank using the phone number from a official letter from them.

What should I think about when using internet on my mobile devices?

Advice on how to protect your mobile device from theft can be found in our Your valuables section.
You can take extra steps to ensure the data your mobile devices contain is kept secure.
Although it is easy to access the internet from a mobile device, it is not without risk. Follow this advice to protect data accessed via your mobile.
Set security protocols to the highest level. Use PIN codes to lock SIMs, keypads and voicemail. Your mobile device can contain personal data.

Take care when charging your mobile on someone else's computer or a charge point. Many chargers are combined with data connection so you could have your data stolen without knowing.
Avoid downloading apps from non-official websites and app stores. They can be used to install malware.
Be aware of others looking at your screen.
Be aware that photos taken from phones have location information on them.
Never respond to spam messages received via SMS or Bluetooth, even to text 'STOP.'
Don't scan a Quick Response (QR) code that looks as if it may have been interfered with. Don't scan it if its stuck over with a replacement or is not from a trusted source. It can leave your phone open to a security attack.

Online gaming

Many people love playing games online. They are regularly logging on, signing up and playing online.

Unfortunately, whenever money or personal data is changing hands online, criminals can be watching. They can be looking for some way to turn the situation to their advantage.
The advice below is intended to help safeguard you and your personal data when gaming.
Whether you use a PC, console, phone or tablet, these steps will help prevent you falling victim to a criminal. This will leave you free to focus on enjoying the game.

Secure your devices

Cyber attacks exploit publicly known weaknesses in devices and software. Keeping your software up to date will help to prevent these attacks from being successful.
Keep operating systems and other software up to date. The easiest way to do this is to turn on automatic updates, if you can.

Account protection

Your gaming account (or accounts) should be well protected with a strong password. This should ideally be one which you don't re-use on other accounts.
You should also turn on two factor authentication if available. This will provide you with an extra layer of protection to prevent someone hacking into your account.

Protect your privacy

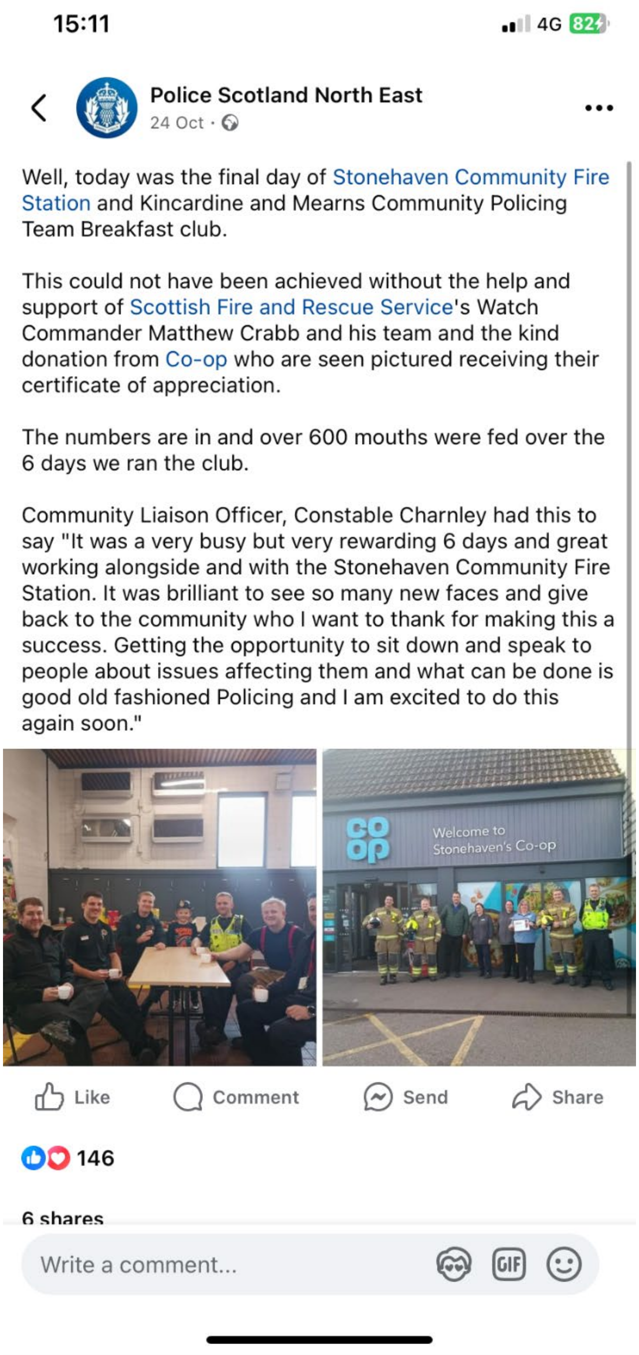
Try to keep the information that you share online to a minimum. Apply privacy settings to ensure your personal data isn't visible to other players.
Do not give out personal information to other players in-game.
When getting rid of your old game consoles and other devices, make sure you follow the NCSC advice on how to delete all your personal data and account details.

Use official sources or stores

Whatever device you are using to play games, you should always verify the source of anything you install. The easiest way to do this is to use official sources and stores.

Cyber attackers try to get round in-game security by persuading you to do something outside of the game itself. For example, a player you don't know may suggest that you install an upgrade and supply a link for the download.
The offer could also come in the form of a well crafted phishing email. This could promise some kind of freebie related to a game you enjoy.
By relying on the official sources for all your software you are much less likely to accidentally install malware on your computer, tablet or other device.

Social Media releases –



Well, today was the final day of Stonehaven Community Fire Station and Kincardine and Mearns Community Policing Team Breakfast club.

This could not have been achieved without the help and support of Scottish Fire and Rescue Service's Watch Commander Matthew Crabb and his team and the kind donation from Co-op who are seen pictured receiving their certificate of appreciation.

The numbers are in and over 600 mouths were fed over the 6 days we ran the club.

Community Liaison Officer, Constable Charnley had this to say "It was a very busy but very rewarding 6 days and great working alongside and with the Stonehaven Community Fire Station. It was brilliant to see so many new faces and give back to the community who I want to thank for making this a success. Getting the opportunity to sit down and speak to people about issues affecting them and what can be done is good old fashioned Policing and I am excited to do this again soon."

Many thanks,

Inspector Rhona Di Meola
Kincardine and Mearns Community Policing Team
12/11/2024