north west leicestershire VALLEY BEAt

Police update APRIL 2020



**NOTICE:**

**Coronavirus (Covid-19): We're asking you please to only call 999 if it is an emergency and 101 if it is urgent. If you can, use our online services. Please only contact us about breaches of the 'stay at home' measures if you feel there is a significant issue or serious breach of the restrictions.**

**• Our information and advice on coronavirus and policing**

<https://www.leics.police.uk/advice/advice-and-information/c19/coronavirus-covid-19/>

**• NHS advice about coronavirus**

<https://www.nhs.uk/conditions/coronavirus-covid-19/>

**• Stay at home measures and other guidance on Gov.uk**

<https://www.gov.uk/coronavirus>

**CRIME FIGURES:**

[**https://www.police.uk/leicestershire/NN43/crime/**](https://www.police.uk/leicestershire/NN43/crime/)

**CYBER CRIME:**

Several million cases of fraud and of computer misuse are reported to the police every year. It's staggering, but even more staggering is that so many of those crimes could have been prevented by making a few small changes in online behaviour.

To avoid becoming a victim of online crime you don’t need to be a computer expert. Developing a few good online habits drastically reduces your chances of becoming a victim of cyber-crime, makes you less vulnerable and lets you use the web safely.

Online fraud, also known as cyber-crime, covers all crimes that:

* take place online
* are committed using computers, or
* are assisted by online technology

To reduce your chances of becoming a victim:

* use a strong password or passphrase, which is at least 12 characters long and contains a mixture of letters, numbers and symbols
* never give personal or sensitive details out online or over email
* make sure all devices have up-to-date anti-virus software and a firewall installed
* keep software and apps regularly updated
* only download from legal, trusted websites
* only open emails and attachments from known and trusted sources
* look for the padlock icon in the address bar when paying for goods or services online – it means the website is trusted and secure
* check the address starts with https:// whenever you’re asked to enter sensitive information online
* avoid using public WiFi hotspots that are not secure or ask you for personal information to access it
* regularly back up your data
* control your social media accounts – regularly check your privacy settings and how your data is being used and shared
* be cautious of internet chats and online dating – there’s no guarantee you’re speaking to who you think
* be extremely cautious if you’re asked for money

**REPORT CYBER CRIME**

If you are currently being subjected to a live and ongoing cyber-attack then please contact us on 101.

If you suspect you’ve been scammed, defrauded or experienced cyber-crime, the Action Fraud team can also provide the help, support and advice you need.

Call Action Fraud on 0300 123 2040 (textphone 0300 123 2050).

**CYBER AWARE:**

Cyber Aware is the UK government's advice on how to stay secure online during coronavirus.

Many of us are spending more time online. Keep yourself and your family secure by following our advice.



***Stay home.***

***Stay connected.***

***Stay Cyber Aware.***

**Our 6 top tips**

1. **Create a separate password for your email**

Your personal email account contains lots of important information about you and is the gateway to all your other online accounts.

If your email account is hacked all your other passwords can be reset, so use a strong password that is different to all your others.

1. **Create a strong password using three random words**

Weak passwords can be hacked in seconds. The longer and more unusual your password is, the stronger it becomes and the harder it is to hack. The best way to make your password long and difficult to hack is by using a sequence of three random words you'll remember.

You can make it even stronger with special characters.

1. **Save your passwords in your browser**

Using the same passwords for all your accounts makes you vulnerable - if that one password is stolen all your accounts can be accessed.

It’s good practice to use different passwords for the accounts you care most about.

Of course, remembering lots of passwords can be difficult, but if you save them in your browser then you don’t have to.

Online service providers are constantly updating their software to keep sensitive personal data secure, so store your passwords in your browser when prompted; it’s quick, convenient and safer than re-using the same password.

1. **Turn on two-factor authentication**

Two-factor authentication (2FA) is a free security feature that gives you an extra layer of protection online and stops cyber criminals getting into your accounts - even if they have your password.

2FA reduces the risk of being hacked by asking you to provide a second factor of information, such as getting a text or code when you log in, to check you are who you say you are.

Check if the online services and apps you use offer 2FA – it’s also called two-step verification or multi-factor authentication. If they do, turn it on. Start with the accounts you care most about such as your email and social media.

1. **Update your devices**

Cyber criminals exploit weaknesses in software and apps to access your sensitive personal data, but providers are continually working to keep you secure by releasing regular updates. These updates fix weaknesses, so criminals can't access your data.

Using the latest versions of software, apps and operating system on your phone or tablet can immediately improve your security.

Remember to update regularly, or set your phone or tablet to automatically update so you don’t have to think about it.

1. **Turn on backup**

If your phone, tablet or laptop is hacked, your sensitive personal data could be lost, damaged or stolen.

Make sure you keep a copy of all your important information by backing it up.

You can choose to back up all your data or only information that is important to you.

FOR INFORMATION ON HOW TO DO THE ABOVE ON YOUR DEVICE VISIT:

[**https://www.ncsc.gov.uk/cyberaware/home**](https://www.ncsc.gov.uk/cyberaware/home)



**OUR DUTY TO PROTECT:**

Over the coming weeks, our policing style remains as one of community policing.

Our preferred style is to

ENGAGE

EXPLAIN

ENCOURAGE

ENFORCE

We will retain a visible presence in neighbourhoods that respects Public Health England guidance around social distancing.

As part of our approach we have published a public pledge to communicate how we are going to police these new measures.

To all in Leicester, Leicestershire and Rutland,

The police have been given new powers to help keep people safe.

As your Chief Constable I would like to make a pledge to you. In return, I ask for your support.

Every day and night my officers and staff go above and beyond to protect our communities.

Every officer at Leicestershire Police knows this as our duty - to protect the people and deal with those who cause harm. We do this by engaging with our communities, explaining and problem solving, and enforcing the law through action when we must.

In this force’s 180 year history we have never faced a challenge like this.

I pledge that my officers will continue to exercise our duty, as we have always done. We will protect you. We will engage positively. We will explain. We will be there when you need help - and we will take action to protect you and others from harm.

I ask for your support in this. Help us to help you. Stay at home and together we will save lives.

**Simon Cole QPM**

**NEIGHBOURHOOD LINK:**

*Neighbourhood Link is a community messaging service from Leicestershire Police that provides news and information about policing activity or initiatives, crime prevention advice as well as major incidents affecting your area.*

*Through this service you can receive messages from your local Neighbourhood Policing Team, local police or, in the event of a major incident or event affecting the whole of Leicestershire, from a partnership of agencies known as the Local Resilience Forum.*

In order to receive messages you will need to register your details. This information will enable us to send you messages relevant to the areas you live and work. Anyone can register, whether you live, work or travel into Leicester, Leicestershire and Rutland. Registration is free and simple to follow.

* Sign up to Neighbourhood Link [**https://www.neighbourhoodlink.co.uk/**](https://www.neighbourhoodlink.co.uk/)
* If you are already registered you can amend your details
* Request a reminder if you have forgotten your username or password
* You can unsubscribe from the service at any time

Neighbourhood Link is not able to receive messages and you should not use it to contact the police. In an emergency always dial 999. An emergency is when a crime is happening, someone suspected of a crime is nearby, someone is injured, being threatened or in danger.

If you wish to contact Leicestershire Police in other circumstances, for example to speak to local police or seek advice on police matters, you can call us by dialling 101 on your telephone.

[**https://www.neighbourhoodlink.co.uk/**](https://www.neighbourhoodlink.co.uk/)

**** untitled2

**BEAT TEAM CONTACTS:**

If you need to contact a member of your beat team and the enquiry isn’t urgent then the easiest way to do this is via Email, you can either do this through the Leicestershire Police website or on the details below:

PC 819 Steve Harrison – [steven.harrison@leicestershire.pnn.police.uk](mailto:steven.harrison@leicestershire.pnn.police.uk)

PC 1391 Adrian Coleman – [adrian.coleman@leicestershire.pnn.police.uk](mailto:adrian.coleman@leicestershire.pnn.police.uk)

PCSO 6867 Kevin Bradley – [kevin.bradley@leicestershire.pnn.police.uk](mailto:kevin.bradley@leicestershire.pnn.police.uk)

PCSO 6178 Nicola Russell – nicola.russell@leicestershire.pnn.police.uk