In the know
Surrey and Sussex

NEIGHBOURHOOD WATCH

Priority: 5 4 3 2 1

CRIME PREVENTION

What Goes Online Stays Online

Everyone has a digital footprint.

Every time you use social media, buy or sell something online, visit any kind of website, send or receive an email, find your way using a mapping app or save a photo to the cloud, you add to your digital footprint. The same goes for downloading music, making Skype calls and using a voice assistant. Every time you post a photo of your children or your friends, you add to their digital footprint too.

Do you ever think about exactly what you're doing online, who can see it and what they could do with it?

We've put together some expert tips to help you minimise your digital footprint, or make sure it's a good one, visit www.getsafeonline.org/yourdigitalfootprint

#yourdigitalfootprint

GET SAFE ONLINE

www.getsafeonline.org

west sussex county council

Every time you use social media, buy or sell something online, visit any kind of website, send or receive an email, find your way using a mapping app or save a photo to the cloud, you add to your digital footprint. The same goes for downloading music, making Skype calls and using a voice assistant. Every time you post a photo of your children or your friends, you add to their digital footprint too.

What happens when you have a digital footprint?
Your digital footprint is part of your online history and can potentially be seen by other people, or tracked and held in a database … or many databases. This is the case even if you are careful with your privacy settings. Here are just a few examples of what could, and does, happen as a result of your online history:

- Companies can target you with specific marketing content on social media and other websites. You could also receive emails, letters or phone calls from these companies.
- Advertisers can track your movement from site to site to gauge your areas of interest.
- Entertainment providers (such as music or films) could target you with unwanted recommendations for content.
- Prospective employers can look into your and family members' background.
- Your child's application for schools, colleges, universities, scholarships, clubs or even sports teams could be rejected.
- You, family members or friends could become the victim of fraud or identity theft.
- Your children could be at risk of criminal activity threatening their online or physical safety.
- Records of your online activity could fall into the wrong hands, including perpetrators of organised crime.
- Tech companies such as browser and search engine providers can track and record what you've searched and viewed. This, in turn, could be shared with other parties including law enforcement agencies.
- You could be refused life, medical, property or vehicle insurance based on information you have shared online.

How to minimise your digital footprint, or make sure it's a good one:

- Don't overshare information about yourself, family members or friends that would be better kept private. That's on social media, websites and apps requesting details and in response to texts and messages.
- Think before you post. Even if your social media privacy settings are set up correctly, there's no guarantee that your posts or photos won't be shared.
- Be aware that every time you visit a website, it's visible to tech companies like website owners, browsers and search engines.
- Read terms and conditions and data privacy policies on websites and apps before providing any personal data or making transactions. What can the providers do with your data, and why would you agree to it? If you're not comfortable with the information being requested, don't provide it.
- Check geolocation settings on mobile devices, apps and cameras. If you don't want anybody to know where you are, or where you have been, disable them.
- Never stop enjoying the many excellent benefits of using the internet, but always bear in mind what digital trail you're leaving, who may be able to access it and how they may be able to use it.

GET SAFE ONLINE
Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit ww.getsafeonline.org. If you think you have been a victim of fraud, report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. If you are in Scotland, contact Police Scotland on 101.

If you're interested in joining Neighbourhood Watch, or want to find out more, visit www.sussexnwfed.org.uk or send an email to enquiries@sussexnwfed.org.uk.

Message Sent By
Derek Pratt (Sussex) (NHWN, Administrator, Sussex)

To reply or forward this email please use the buttons below or these links: Reply, Rate, Forward / Share.

Reply | Rate | Share | Print | Settings

To login to your account, click here, To report a fault, click here

neighbourhood ALERT
Informing & Listening to Communities

CYBER ESSENTIALS PLUS

You are receiving this message because you are registered On In The Know - Surrey and Sussex. Various organisations are licenced To send messages via this system, we call these organisations "Information Providers".

Please note that this message was sent by Neighbourhood Watch and that Neighbourhood Watch does not necessarily represent the views of In The Know - Surrey and Sussex or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking here, or you can unsubscribe completely, (you can also review our terms and conditions and Privacy Policy from these links).

This e-mail communication makes use of a "Clear Image" (gif) to track results of the e-mail campaign. If you wish to turn off this tracking for future e-mails, you can do so by not downloading the images in the e-mail itself.