Watching Brief

The Canterbury & District Neighbourhood Watch Newsletter

Registered Charity No 1078269

2020 – Issue 3 (Jul - Sep)

Chair's Message – David Hayward BEM

Greetings to everyone – in the hope that as many of us as possible are managing to keep safe and well in what, at the beginning of this year, would have been considered as impossible-to-imagine national and global health conditions. At the same time, I send my sympathies to those who have not fared so well. As an Association we continue to work to support all our members as best we can – and, as can be seen from some of the content in this latest issue of "WB", NHW has clearly been responsible for helping to promote even greater feelings of good "neighbourhoodliness" than might have already existed. Notwithstanding the several 'caveats' contained in this issue of "WB" around staying safe whilst using various form of 'new technology' it's interesting that some such means are also serving a very useful and helpful purpose in this promotion of closer community togetherness, with increasing reported use of *WhatsApp* and emailing in particular. (Needless to say, privacy issues in respect of emailing need to be enacted, perhaps especially the use of "bcc" when sending group emails unless otherwise agreed by all recipients). One way in which this new technology came to our rescue was in respect of holding our "virtual AGM" which, as described below, has allowed us to continue to function as an Association. This concept was proposed and undertaken by our continuing Vice Chair, Neal Fowler, and is being seen as a precedent for other Kent District Associations – so, many thanks to him not just for that but also for sorting out our new website and, of course, producing our "WB". Those of you who studied our AGM accounts for 2019 will have seen that we were already in quite a sound financial position. This has now been enhanced by the receipt of an 'indirect' legacy of just over £10,000.00 from a Mr George Pinto – a retired resident of East Kent, tragically was killed in a road accident in 2019. He clearly had connections with the now closed Canterbury Crime Prevention Panel and left them some money to help them to continue their work. As some of you will already know, all of the CCPP's assets were kindly transferred to us on their closure and Mr Pinto's bequest has now also been able to be passed on to us. Clearly this helps even further to secure our future, as well as give us opportunities to consider various new NHW projects within the District. And finally – a very warm welcome to Duarte Figueira, who has just joined our Committee as a co-opted member, and best wishes in as much as is possible to keep staying safe and well.

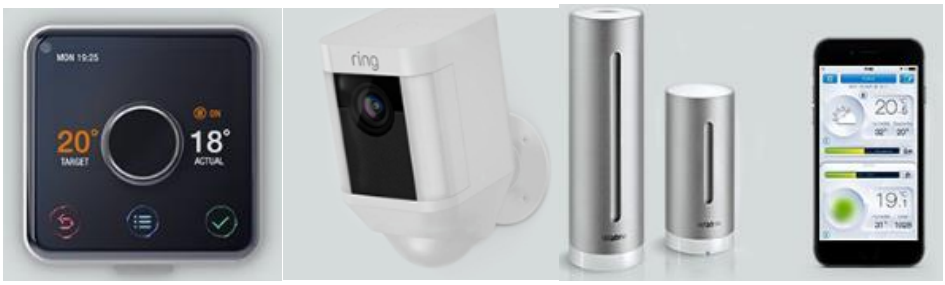
All Systems Go For New Website

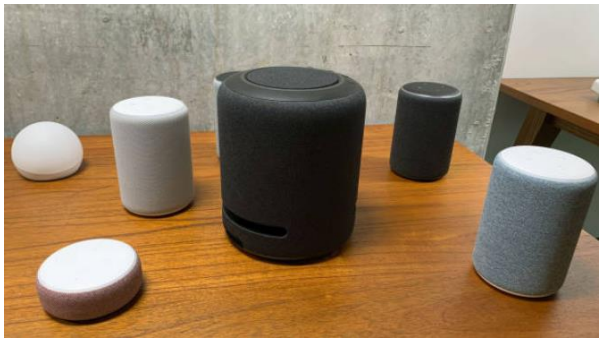
Welcome To Canterbury & District NHW Association

As mentioned in the last issue of Watching Brief we now have a new website which can be accessed via the following URL www.canterbury-and-district-nhw.org The new site provides all of the information, guidance, advice and news items that were on the old webpage but everything is more interactive and easier to find/navigate. Two items added very recently are our new Health & Safety Statement, which you'll find on the 'Policy Documents' page and this year's insurance policy, which includes Pubic Liability cover for all C&DNHWA schemes. There is also a page providing information about recent scams that have come to our attention from Coordinators. As with all newly published websites, it will take a short while for your favourite search engine to find us quickly, so for a start you may have to enter our URL directly into the address line of your search page. Once you have found our site please save it as a bookmarked page so that you can return effortlessly to it in the future. For those schemes which have websites of their own (and there must be some) please add our site to your list of linked pages – and also let us know your URL so that we can add it as a link on our site, if of course you think that would be helpful.

The Taming Of The Shrewd Devices

What technology is increasingly omnipresent in your home, office, smartphone, watch and can control almost everything, including your light bulbs, fridge, garage door and air conditioning? The answer, of course, is 'virtual assistants', i.e. **Amazon Alexa** / **Google Home** (other competitors also exist). The number of virtual assistant devices is rising exponentially around the world, together with the range of 'smart' devices they can control. The main reason is that they are very useful. They help to automate our lives, saving us time and effort. And using a voice-activated assistant to get a world news update is a much *smoother* experience than tapping a search term into a laptop or unlocking your phone. As with many new technologies there are concerns. The most prominent of these are invasion of privacy and potential hacking. This article will provide some basic advice to enable you to control these devices better. On the personal privacy side, these concerns have some justification. Last year, Amazon admitted that it stores and uses recordings from a diverse range of customers. This (apparently) *"helps ensure Alexa works well for everyone"….* and *…."may be used to develop new features and help improve our services. Only an extremely small fraction of voice recordings is manually reviewed."* You can disable this setting, left on as a default, to avoid such intrusion. Go to the '**Manage content and Devices**' page on your online Amazon account, choose '**Privacy Settings**' and scroll down until you reach the '**Help Improve Alexa**' section and turn the tab to 'off'. You will get a warning that, if you do, voice recognition and new features may not work for you. You can also listen to your voice recordings on your Alexa app or Amazon online account on the '**Privacy Settings**' page. These transcripts of recordings sent to Amazon's servers can be deleted individually or completely. To enable deletion by voice you can also change the relevant tab so you can say to your Echo "*Alexa, delete everything I said today*". If you do, Amazon will warn you that anyone with access to your Alexa device can delete anything said. With Google Home, the voice assistant is built into many Android smartphones. To set audio recording preferences on your phone or tablet, open '**Settings' > 'Google Account' >** tap **'Data & Personalisation'** at the top **>** under **'Activity Controls'** select '**Web & App Activity'** and then check or uncheck the box next to "**include voice and audio recordings**". You can review your voice transcripts from Google Assistant by navigating to and logging into your Google Account. Then on the navigation panel, click **'Data & Personalisation' > 'Activity controls' > 'Web & App Activity' > 'Manage Activity'.** You can look at and delete your past activity. Any files with an audio icon will include a recording. You can also instruct Google Assistant to delete activity from your account, such as by saying, "*Hey Google, delete my last conversation*." Concerns whether virtual assistants can be hacked are real. Last year, security researchers at product review giant, CNET, discovered that some malicious skills (which have since been removed) allowed the relevant app to listen in on speakers – See https://www.cnet.com/news/alexa-and-google-voice-assistants-app-exploits-left-it-vulnerable-to-eavesdropping/ It remains important to be careful when downloading apps, such as by reading trusted reviews. As ever, common sense applies. Risks of hacking can be minimised by turning off the microphone when you don't plan to use your device. It is also important not to place the assistant near a window or location easily accessible from outside. Apart from minimising the risk of conversations being overheard it also makes it less likely that your device (and through it any smart devices) could be remotely accessed. Locating your device close to your TV runs the risk that something is heard by the virtual assistant which causes it to activate, recording you as well as interrupting your viewing! For those enthusiastic about voice assistants, the concerns above may seem like technophobic paranoia. For the more cautious, the enthusiasts may appear complacent. For those considering investing in an Alexa-enabled, Google Home or similar device the good news is that the concerns can be largely mitigated with a modicum of effort. Virtual assistants would only be a serious threat to privacy if they were imposed on us — but they have to be 'invited' into your home. If ownership of a virtual assistant would keep you awake, worrying about being overheard, perhaps it's not for you. Any device which is hackable is also eminently protectable if you take sensible steps, so grip your virtual assistant challenge with confidence!





Watch Out For Covid-19 Scams As The Test And Trace Service Starts

With the NHS as coronavirus contact tracing system barely out of the blocks the authorities are already warning users to be on their guard against scammers' probable attempts to con people into handing over personal details to them. Contact tracing works by asking people who have tested positive for the virus to share the details of others who they have been in contact with and whom could have caught it from them. This is exactly the kind of information fraudsters want and need in order to trick people out of their money, making the service an ideal target. Here, we explain how the official NHS contact tracing service works and how you can tell a real message from a fake one.

If you have coronavirus symptoms you can get tested. If your test is positive you'll be contacted by NHS England by text, email or phone. The NHS England Test and Trace service will only get in touch with you for one of the following two reasons either: **1. You have tested positive for the virus** or **2. You've been in contact with someone who has tested positive for the virus.**

If you test positive for the virus, you'll be contacted within 72 hours of taking the test. Genuine texts, calls or emails from the NHS service won't ask you for any personal details upfront. You'll be given a unique ID number to log in to the NHS England Test and Trace website. The only official web address for the NHS Test and Trace service is: https://contact-tracing.phe.gov.uk/ Once you've logged in using your ID, you'll be asked to enter some basic information about yourself including: your name, date of birth, current address, the names of the people you live with, places you've recently visited, and the names/contact details of people you were in touch with around 48 hours before you developed symptoms. If you can't access the website, you'll be asked to give these details over the phone. **If you get a call about testing positive for coronavirus, but you haven't taken a test in the past few days or have never taken a coronavirus test, then the call isn't real and is very likely to be a scam.** A smartphone app that will alert people when they have been in contact with a coronavirus infected person is still being trialled on the Isle of Wight. It's not currently available for the general population, so don't download any apps that claim that they can provide this service until official notification about availability is released.

If you've been in contact with someone who has tested positive for the virus the NHS will contact you and you'll be asked to self-isolate for 14 days. You'll be given advice on how to do this, what symptoms you should look out for and what to do if you develop the illness. You won't be asked for any other personal details or payment information in this kind of call or message. And, crucially, you won't be asked to pass on the details of anyone you've been in contact with either. This is because unless you have tested positive or developed symptoms, there is no need to notify anyone you've been in touch with at that stage. It's a red flag if you're asked to hand over this information to a caller or by replying to a message. Check the caller or sender's details The NHS Test and Trace service will only come from one verified NHS number: **0300 013 5000**. The following video shows how to avoid being scammed https://www.youtube.com/watch?v=FgNjAWU-69s&feature=youtu.be

If you've received a message or call that you think is a scam you can report it to Action Fraud, the national fraud reporting centre at www.actionfraud.police.uk/. If you can take down any details such as numbers or email addresses, that will be useful. If you've given away payment or bank details to a potential scammer let your bank know as soon as possible. They'll be able to help you protect your accounts. If you've shared other personal details, keep an eye out for unexpected bills or invoices addressed to you. Check your credit report regularly for any new accounts that you haven't opened.

No Marriage Made In Heaven!

Marriage Allowance is a tax break for those who are married or in a civil partnership with a relatively low income. It allows for the transfer of part of the income tax personal allowance from one person to another, reducing the household's overall tax liability, which clearly could help couples whose salaries have been adversely affected by the coronavirus pandemic, but care should be taken about how applications are made. For the 2020-21 tax year taking advantage of the Marriage Allowance could save £250. However, claims can also be backdated for up to four years, resulting in a potential saving of £1,000 or more. Normally the allowance is agreed, without cost, through contacting HMRC (the Government Tax Office) but several companies offer to apply for you, for a fee. One such company, Marriage Allowance Claims Ltd, charges 42% commission (plus £24 and VAT). The company is registered at Companies House, but like all claims-management companies it doesn't need to be registered with the Financial Conduct Authority and as a result is effectively unregulated. This can make for difficulties in cases of dispute, of which there have been many, it seems, because the company's advertising has lead consumers into thinking that they are dealing with HMRC directly. So if you think that you might be entitled to claim the Marriage Allowance, the advice is to contact HMRC by signing into your Government Gateway account. If you don't already have an account, you can create one at https://www.gov.uk/log-in-register-hmrc-online-services

Cop This!

In our modern world so much business is now conducted on-line, and the impact of Coronavirus has simply served to increase the flow of electronic bank transfers, contractual agreements and so much more. So it's not surprising that fraudsters have increased their efforts to muscle-in and take advantage. Warnings abound about password safety, and many of us are careful to comply with advice in order to reduce risks to bank accounts. But lapses in email security could be equally lucrative for criminals, as one of our own coordinators found out recently! She had been conversing, via email, for some weeks with her trusted, legitimate, contractor who was in the process of completing major work at her home. So when an email arrived asking for the payment of the next instalment of funds into a bank account to continue the project the request was actioned promptly. It was only a few days later, when the contractor phoned to ask why the payment hadn't been made that alarm bells rang. Checking back, the original email request looked completely normal BUT the back account details were not those of the contractor – his email account had been hacked allowing the fraudster to 'eaves drop' for long enough to know exactly when to lay the trap and provide false account details. The bank was immediately contacted and the contractor changed his email password. This should have prevented a further 'attack' but the fraudster, realising he/she had been rumbled, tried a different approach to get more money from the victim. The contractor's email address contained the word 'driveway', so the fraudster created a new email account which mirrored the contractor's email in every respect except the 'w' in 'driveway' was changed to 'vv' (two vees) making 'drivevvays' look extremely similar to 'driveways'. Fortunately, with the victim's guard already raised, the trick didn't work but it shows the lengths to which criminals will go to pursue a victim once they have successfully been duped the first time. The police and Fraud Action have, of course, been informed but the fraudster has not been identified – yet. This type of fraud has plagued the banking system for quite a while but now, with the introduction of a new security check implemented by most banks, called **Confirmation of Payee** (CoP), it should become much harder for the criminals to pull-off in future. The CoP system is used when bank customers set up a new payee from their account. It provides a check of the name of the person or organisation that will receive the payment to ensure that the details are correct before allowing the transfer of funds. Some financial institutions ask the customer to actually confirm that the details are correct before proceeding, which provides even more peace-of-mind. Unfortunately, in the case highlighted above, the new system came into effect just 5 days too late but hopefully it will be the last time that that fraudster manages to scam anyone by the same trick, in this country anyway. You should easily be able to see how the CoPs system works at your bank/building society by going to your account on-line. CoP should apply to payments like one-off bills, standing orders, and CHAPS payments.

Virtual AGM Report

Like so many other organisations C&DNHWA has had to adapt following limitations imposed as a result of Covid-19. So it was that we had to cancel our scheduled annual conference and AGM in March. But with a need to complete the year's business, and elect a Committee to continue work this year, we had to find a way forward. A 'virtual' AGM, conducted electronically by email provided the solution, and the response from our coordinators and deputies did not disappoint. About 33% of eligible Members returned their voting forms, which provided ample response to ensure that the AGM quorum was met. The following business was agreed by the 'meeting':

- The minutes of the 2019 AGM were unanimously agreed, as were the accounts for 2019;
- Members of last year's Committee, or at least those willing to stand again, were re-elected en-bloc in accordance with the Constitution. And two new Members (both of whom were co-opted Members during 2019) were elected as full Committee Members;
- Also unanimously agreed was amended wording to our Constitution, which now provides ability for co-opted Committee Members to fill vacant places between AGMs and also, officially, have voting rights within that group. Their previous capacity to do so was unclear, which raised potential for difficulty in getting Committee business completed when some fully elected Members were not available to attend meetings.

With Coronavirus restrictions likely to be in place for some considerable time, the new Committee undertook its first meeting with the aid of Zoom video conferencing. The first meeting of the year elects Officers, which is vital for conduction of future business. **Association Officers for the coming year can be confirmed as:** Chair – David Hayward; Vice Chair – Neal Fowler; Secretary – Rachel Pearson (a new Committee Member); and Treasurer – Val Horne (also newly elected to the Committee). The meeting also welcomed Duarte Figueira (as a new co-opted Member), before proceeding to the agenda, and discussion of several key issues including agreement of a Health & Safety Statement and a domain name for our new website – see article on page 1 for more information.

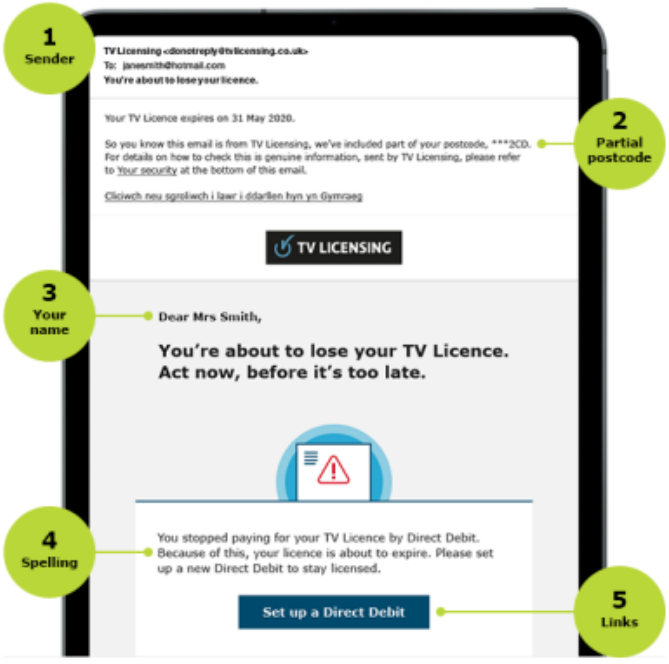
Flags, Felicitations and the Fickle-Face of Freedoms

If ever there was a crisis (in modern times) to bring out both the very best and worst in the population it has to be Coronavirus, and two recent reports serve to highlight examples in both camps! On the plus side the Government's 'lockdown' measures have led to a surge in neighbourliness, according to a new study released today by **Co-op Insurance**, as people look out for the vulnerable and talk to those next door more than ever before. Almost three quarters (72%) of UK adults, it seems, can now identify which of their neighbours are vulnerable and over a quarter (26%) checked in on them regularly during the crisis. And togetherness, at a safe social distance, was the theme of the 75th VE Day celebrations too with many of our NHW schemes participating in a totally new kind of street party. The theme of neighbourliness continued during this year's NHW week. The 'Let's Stay Connected' campaign ran between 7th – 13th June and commenced with 'The Big Virtual Lunch' – which provided simple ideas for staying connected, even during Covid-19 lockdown. See https://www.ourwatch.org.uk/letsstayconnected More disturbingly, it was increasingly evident (according to consumer watch-dog ***Which?***) that unscrupulous sellers were exploiting the coronavirus crisis, using the shortage of essential products to vastly inflate prices. This prompted *Which?* to ask us all to help bring this unjustifiable behaviour to an end by reporting examples of it to their new on-line price-gouging tool – to be found on their website at: https://www.which.co.uk/tools/report-price-gouging/

As UK citizens we enjoy considerable freedom of choice – to do the right thing, or the wrong one! For so long as the majority choose the former over the latter we are on the right path and there is hope! – Ed

Licence To Scam

TV licences have been provided free of charge the over 75s for many years but some while ago the BBC announced that this would be ending for most people this year. Originally it was planned to make the change from the end of May but complications of the Coronavirus pandemic has now seen the date move to 31 July, when a new scheme commences for that age group. Under the new scheme, anyone aged 75 or over receiving Pension Credit will still be eligible to apply for a free TV Licence. Pension Credit can be in the name of the licence holder, or in their partner's name if they are a couple living at the same address, otherwise the TV Licence will need to be paid for. Those that turn 75 between the end of May and 31 July can apply for a free short term licence. The change of implementation date for the new system provides perfect opportunity for scammers to target elderly people, some of whom, inevitably, will be confused about the changes and the date on which the new system starts. Already one Coordinator from Herne Bay has received an email purporting to be from TV Licencing Authority (TVLA) demanding payment of £11.99 within 2 days because, they claimed, that the expected payment for the new licence had not been made by the customer's bank. The email looked genuine, seemingly coming from the usual 'donotreply' email address of the TVLA – but there were plenty of tell-tale signs to indicate that it was a scam, if of course you know what to look for! Most obviously the link that the scammers wanted victims to use to confirm details / make payment was 'dallasprint.com/signupmails' – ascertained by hovering the mouse over the 'update your details' link **without pressing any mouse buttons** – clearly not the TVLA. Genuine emails from TVLA will be addressed to the customer by name, not by their email address, and / or they will contain part of the customer's postcode. Also the TVLA never ask for card details UNTIL you've signed in using your licence number, surname and postcode.



Getting In Touch with C&DNHWA & Useful Contacts:

You can reach us through our website www.canterbury-and-district-nhw.org which also contains lots of useful information, advice and links to other organisations, or by email at canterbury.nhw.association@gmail.com You can now follow us on Facebook too https://www.facebook.com/CanterburyDistrictNeighbourhoodWatch/

Editorial & Layout – Neal Fowler