

Report to Communities, Highways and Environment Committee

18 November 2022

Digital Crime

Report by Assistant Director (Communities)

Electoral division(s): All

Summary

The scale of how digital risk and harm impacts safeguarding on a national and local level is unprecedented. The consequences of which result in ever increasing pressure on local services. It is essential that the Safer West Sussex Partnership continues to provide strong and effective partnership response, to minimise harm, mitigate demand pressures and robustly meet existing and future challenges. The partnership is and will remain committed to finalising the county wide digital and inclusion strategy and the associated delivery plans and wherever possible increasing the resource capacity focussed on this growing critical agenda.

Focus for Scrutiny

Scrutinise the Safer West Sussex Partnership arrangements for Digital Safety in West Sussex to obtain a more coherent and detailed picture of the threats, harms, risks and vulnerabilities that impact our communities and residents. In particular, that the Committee:

- (1) Supports the current partnership approach to reducing harm sustained or enabled via digital devices/platforms.
 - (2) Asks all members to sign up to and publicise the monthly staying safe online e-newsletter and follow the associated social media accounts.
 - (3) Considers opportunities when engaging with communities to raise awareness of and promote the services provided by the Safer West Sussex Partnership.
 - (4) Utilises networks to share wider public messages to increase safety and raise awareness of new developments.
-

1 Background and context

International overview

- 1.1 The global nature of the internet, ease of communication, the fast-paced nature of technology, including the fact that connected devices are integral to

people's lives, means the online world has added complexity to safeguarding and protecting children and vulnerable adults.

- 1.2 Illegal and unacceptable content and activity is widespread online, the most serious of which threatens national security and the physical safety of children.
- 1.3 Online platforms can be, amongst other things:
 - A tool for abuse and bullying.
 - A means to undermine democratic values and debate, including mis and disinformation.
 - Used by terrorist groups to spread propaganda and radicalise.
 - A way for sex offenders to view and share illegal material, or groom and live stream the abuse of children.
 - Used by criminal gangs to promote gang culture and incite violence.
 - Increasingly used for criminal gain.
- 1.4 Additionally, platforms can be used for other online behaviours or content which may not be illegal but may be detrimental to both children and adults, for example:
 - The potential impact on mental health and wellbeing.
 - Echo chambers and filter bubbles driven by algorithms; being presented with one side of an argument rather than seeing a range of opinions.
- 1.5 It is widely recognised that the internet was never designed with children in mind; many protective measures are reactive and inconsistent rather than proactive. Historically, global technology companies have largely self-regulated in relation to content, contact and conduct of users, seemingly only responding when there is public outcry.
- 1.6 Whilst there are statutory measures to prevent or remove content that is illegal, this is less clear when it relates to content that is legal but potentially harmful. Most interactive online services have age restrictions, commonly age 13, to comply with advertising laws (the U.S. Children's Online Privacy and Protection Act, and in the UK the General Data Protection Regulations, GDPR), yet very few have effective age-verification processes or parental controls. Furthermore, potentially harmful content doesn't just relate to children, it can significantly affect adults too. For example, misinformation and disinformation related to COVID-19 or the efficacy of vaccines, election campaigns and much more.

National Overview

- 1.7 The UK has started to lead the way in this area with the introduction of the [Age-Appropriate Design Code](#). Often called The Children's Code, this is a statutory code of practice under the Data Protection Act 2018 brought into legislation in September 2020 which places a baseline of protection automatically by design and default. However, the Children's Code is UK legislation; the internet is global. Whilst everyone is at some level of risk, front of mind for any service delivery should be protections for those who are vulnerable, children and adults alike. Evidence is clear that those with a real-world vulnerability are not only more likely to experience online risks but suffer more than their non-vulnerable peers.

- 1.8 In April 2019, the [Online Harms White Paper](#) was published proposing that all technology companies, big or small, will have a duty of care to their users commensurate with the role those companies play in our daily lives. After a period of consultation, the Government released their full response to the white paper on 15 December 2020 and on 12 May 2021 the Government released the draft Online Safety Bill.
- 1.9 [The Online Safety Bill](#) establishes a new regulatory framework encompassing plans for a system of accountability and oversight for technology companies which moves beyond self-regulation and with the aim of preventing harm to individuals in the United Kingdom. This framework will make clear to companies their responsibilities to keep users in the UK safer online by imposing duties of care in relation to illegal content and content that is harmful to children, whilst also imposing duties on providers to protect rights to freedom of expression and privacy. Providers of user-to-user services, which includes a broad range of businesses including social media platforms, dating apps, online marketplaces etc, which meet specified thresholds, will have additional duties imposed specifically in relation to content that is harmful to adults, content of democratic importance and journalistic content.
- 1.10 An inquest took place during September 2022 about the death of 14-year-old Molly Russell. Coroner Andrew Walker concluded that Molly Russell "died from an act of self-harm while suffering from depression and the negative effects of online content". He continued to say that Molly was "exposed to material that may have influenced her in a negative way". In some cases, the content was particularly graphic, tending to portray self-harm and suicide as an inevitable consequence of a condition that could not be recovered from".
- 1.11 It is clear from the Molly Russell inquest that considerable areas within the field of online safety need to be addressed. As well as this, it has brought into discussion the Online Safety Bill and how the Government will ensure children and young people are efficiently protected online. Following the inquest Sir Peter Wanless, NSPCC CEO, has said, "Tech companies must expect to be held to account when they put the safety of children second to commercial decisions. The magnitude of this moment for children everywhere cannot be understated."
- 1.12 During 2020/21 Childline delivered more than 73,000 counselling sessions about mental health, and in the same period there were 24,200 counselling sessions about suicidal thoughts or feelings.
- 1.13 The serious and organised crime landscape has changed drastically in recent years - in large part due to advances in technology. Criminals quickly adopt and integrate new technologies into their modus operandi or build brand-new business models around them. The use of new technologies by organised crime groups (OCGs) has an impact on criminal activities across the spectrum of serious and organised crime. This includes developments online, such as the expansion of online trade and widespread availability of encrypted communication channels, as well as other aspects of technological innovation. Technology has become a key component of most, if not all, criminal activities carried out by OCGs and has afforded organised crime with an unprecedented degree of flexibility.

Research and Reports

- 1.14 The [Internet Watch Foundations \(IWF\) 2021 annual report](#) highlighted some key concerns in relation to child sexual abuse material.
- Sexual abuse imagery of girls is increasing.
 - The IWF took action to remove over a quarter of a million URLs (Uniform Resource Locator - a URL is the address of a given unique resource on the internet) which contained images or videos of child sexual abuse.
 - Over 182,000 URLs contained images and videos of self-generated material, an increase of over 374% of pre-pandemic levels.
 - Sexual abuse imagery of children aged 11-13 is most prevalent, accounting for 70% instances identified in the past year.
- 1.15 New data released by the IWF shows almost 20,000 webpages of child sexual abuse imagery in the first half of 2022 included 'self-generated' content of 7- to 10-year-old children. That is nearly 8,000 more instances than the same period last year. When compared to the first half of 2020, when the UK entered its first Covid lockdown, there has been a 360% increase in this type of imagery of 7- to 10-year-olds.
- 1.16 The internet gives young people unprecedented opportunities to engage with the world around them and plays an increasingly important part in their education and learning. For some young people, and in particular those who are lesbian, gay, bi and trans (LGBT), the internet also provides a way to reach out to others having similar experiences to them. A report published by [Stonewall, Staying Safe Online](#) states that nine in ten LGBT young people (90 per cent) say they can be themselves online, and nearly all LGBT young people (95 per cent) say the internet has helped them find positive role models. In this sense, it can be a great source of hope for those who have few LGBT peers around them at school, college, at work or in their community. It can provide opportunities for unsafe behaviour, with two in five (39 per cent) young people aged 13-19 having met up with someone they contacted and talked to online. Of those, nearly one in five (18 per cent) did not tell anyone they were meeting up. For those who are LGBT, the risks are often even more pronounced – either because the information they are given around internet safety doesn't specifically address LGBT issues, or because they're afraid they will be judged or outed for their sexual orientation or gender identity if they ask for advice. Homophobic, biphobic and transphobic abuse is rife online, with nearly all LGBT pupils being exposed to offensive content about LGBT people.
- 1.17 Vulnerable young people are more at risk online. The [Internet Matters Refuge and Risk report](#) states that vulnerable young people experience high levels of cyberbullying, cyberaggression and manipulation or coercion. Their greater exposure to unknown people, as they seek out new friends or 'people like me,' tends to make them targets. Age, social isolation and digital competence all contribute to the extent of the online risks young people face.
- 1.18 The [Violence Against Women \(VAWG\) and Girls Code of Practice](#) guidance has been created due to the high prevalence of VAWG perpetrated in the digital sphere. This includes technology-facilitated abuse (activities carried out with

the use of technology and communication equipment, including hardware and software) enabling abusers to stalk, harass, survey, and control victims. The obligations placed on regulated providers as set out in the Online Safety Bill, are to prevent harm against adult and child users in this context. It is a 'living' document that will continue to evolve as the Online Safety Bill progresses through Parliament.

- 1.19 The [United Nations](#) (UN) recent research explores the intersection between gaming and violent extremism. The report notes increasing evidence that extremists are using gaming-related content and are present on gaming or gaming-adjacent platforms. It is documented that extremists are using gaming-related content to produce their own games, modify existing games, making use of in-game chats/platforms, using gaming references and finally making use of top-down/bottom-up gamification practices to increase the familiarity and attractiveness of their propaganda/ideology. Gaming spaces operate in a very-similar way to social media platforms where users discuss a variety of topics they are interested in, and therefore it's reasonable to expect that political views are taken into the spaces and then exploited by extremist individuals. This was noted to be the case with both the Christchurch and Halle terrorist attacks, where the individuals understood themselves to be part of gaming communities and tailored their livestreams and manifestos accordingly. In addition, gaming spaces are more prone to being exploited by extremists through the lack of moderation, potential audience reach, networking opportunities and customisation options.
- 1.20 In data terms, the research by the UN recorded in respect of gaming-related activities, participants (of which there were 644) generally used more than one platform, including Discord (83%), Twitch (45%), YouTube (39%) and Reddit (24%). A small percentage (less than 1%) used 4chan, Instagram, Slack, Skype, and Snapchat, indicating that these spaces are generally not of interest for most gaming-related activities. The toxicity in gaming communities was the most prominent complaint by participants, with a note that this has increased since the start of the Coronavirus pandemic. 85% of research participants remarked they had witnessed toxic behaviour when gaming. 30 to 34% of participants stated they had witnessed "a great deal" or "a lot" of misogyny, racism/xenophobia, or homophobia, only 15% to 16% said they had witnessed similar levels of extremism, antisemitism, or islamophobia. This apparently confirmed some of the thoughts expressed in focus groups that casually racist, heteronormative, and misogynistic language often appears in open and public gaming spaces, but rarely targets individuals based on religious identity or is explicitly extremist in nature. This does identify that misogyny, racism/xenophobia and homophobia are regular occurrences in gaming spaces and may be used as a springboard for extremist actors.
- 1.21 [Europol's Internet Organised Crime Threat Assessment \(IOCTA\) 2021](#) states that COVID-19 fuelled the increase of cybercrime in all its forms. In this year's report, the impact of the COVID-19 pandemic remains visible. The accelerated digitalisation related to the pandemic has significantly influenced the development of several cyber threats, including ransomware affiliate programs that enable a larger group of criminals to attack big corporations and public institutions by threatening them with multi-layered extortion methods such as distributed denial-of-service (DDoS) attacks. Mobile

malware is evolving with criminals trying to circumvent additional security measures such as two-factor authentication. Online shopping has led to a steep increase in online fraud. Explicit self-generated material is an increasing concern and is also distributed for profit. Criminals continue to abuse legitimate services such as virtual private networks (VPNs), encrypted communication services and cryptocurrencies.

- 1.22 Online fraud puts increased pressure on local Public Health & Social Care services. Research produced by [AGE UK](#) identifies that people defrauded in their own homes are 2.5 times more likely to either die or go into residential care within a year. The impact of being a victim of fraud not just being a financial one, but also encompassing the physical and mental health related effects of being a victim. National Trading Standards have reported of some cases where fraud victims have considered, attempted, or committed suicide. The threat from fraud has almost certainly increased as a result of COVID-19. The pool of potential victims living and working online is larger than ever and additional vulnerabilities are created through isolation or financial instability. The pandemic and most recently the cost-of-living situation, has become a key 'hook' and narrative for offenders.

West Sussex Overview

- 1.23 The current Safer West Sussex strategic intelligence assessment identified that reports of fraud had increased during 2021 compared with 2020. This reflects the national picture where fraud and computer misuse rose exponentially by 54% during 2021.
- 1.24 A quarterly fraud report is produced by Sussex Police. The report enables partners to better understand the impact of fraud locally and facilitates better focusing of prevention activity and resource. The report identifies top fraud types, amounts lost, any trends and victim demographics.
- 1.25 Data from these reports during 2021 identifies that online shopping and auction fraud and courier fraud/impersonator fraud were the highest reported fraud types in West Sussex. This trend has continued into the first half of 2022 with courier fraud/impersonator fraud being the highest reported fraud type.
- 1.26 £21.4million was lost due to fraud in West Sussex during 2021 (figures from reported action fraud reports).
- 1.27 Dating and romance fraud has been consistently one of the most reported fraud types in West Sussex over the past few years (in the top five most reported). Recent data from 1st January 2022 – 28th September 2022 shows that there have been 131 reports of romance fraud (12% of all fraud reports) resulting in a £1.82 million total loss, £21,360 average loss of those with a loss. The scale of Romance Fraud and the financial and emotional impact on victims is enormous and it is the fraud type with the highest links to suicide. Fraudsters set up fake profiles on legitimate dating sites, appear charming, sincere and loving and eventually the conversation turns to requests for money. These scams are usually perpetrated from abroad meaning most relationships rarely result in a face-to-face meeting. Romance Fraudsters usually pretend to be coming to the UK, but something prevents them like an accident, issue at customs etc. We sometimes see victims travel to Gatwick

and call police to report a partner missing as they haven't arrived on their intended flight.

- 1.28 The County Council recently undertook a county-wide parent/carer online safety survey, with the aim of better understanding the local picture in terms of how parents & carers feel about their child's digital resilience. It will also help to inform safeguarding professionals and shape future digital safety resources. The results and analysis of the survey will form a report due to be completed and shared with partners in December 2022.
- 1.29 For online Radicalisation and Extremism, whilst we cannot share local Channel data, we are seeing children and young people as an area of concern, with partners (particularly schools) noting concern with their student's use of the online space and the risks inherent in this. As noted from the national research, Discord is one app that we have seen flagged up in several cases of concern. Increasingly local referrals into Prevent involve an online element, such as accessing extremist material on websites and forums, and contacting others on encrypted and gaming platforms. Self-Initiated Terrorism is an increased concern in the UK and accessing extremist material online is a key driver for SIT self- radicalisation. Online platforms are increasingly used by those promoting extremist narratives to influence and engage vulnerable people. Groups are documented as increasingly using misinformation and propaganda to engage and radicalise individuals in easy to access mainstream online spaces.

West Sussex Partnerships

- 1.30 The current priorities for the Safer West Sussex Partnership are;
- Violence and Exploitation
 - Domestic and sexual violence and Abuse
 - Substance misuse
 - Social inequality and hate crime
 - Digital Safety
 - Preventing Radicalisation and Violent Extremism
- 1.31 Digital Safety is a cross cutting theme across all of these priorities and our response is focussed on three priority groups which are:
- Children and Young People
 - Working Age Adults
 - Older Residents
- 1.32 Strategic responsibility for the partnership response to Digital Safety sits within the Community Safety and Wellbeing Service, with the Digital Safety Lead Officer currently reporting to the Head of Community Safety and Wellbeing.
- 1.33 In West Sussex the partnership response is soon to be coordinated through a newly formed Digital Safety Steering Group.
- 1.34 The current partnership network includes Citizens Advice Bureau, Carers Support, Turning Tides and Parish Councils. With some of the key partnership activity currently being driven and delivered by Sussex Police, Victim

Support, South East Regional Organised Crime Unit, NHS Sussex, WSCC Libraries, WSCC Trading Standards, Neighbourhood Watch and District & Borough Councils.

West Sussex Partnership Response

- 1.35 The County Council has commissioned and worked with Get Safe Online (GSO) for the past 6 years, delivering their online safety programme across the county. Originally a police-based programme, West Sussex was one of the first counties to deliver the GSO programme at a local government level. The programme includes engagement work at local events, training for professionals and communities, access to a range of resources and monthly themed campaign materials.
- 1.36 The partnership promotes on-line safety at local events including the Worthing Fire and Rescue Service Open Day, Crawley 999 Event, Crawley Shopping Centre and Freshers Fair days at Chichester University sites. It also provides a wide range of resources to support key safety messaging and training including a partners website containing leaflets, guides and presentations. The County Council have worked with GSO to produce local resources including posters to support residents' safety and for parents and carers to support their children to be safe online. The GSO monthly campaign material is widely utilised and shared via an extensive partner network.
- 1.37 In September 2021 West Sussex built on the strong partnership relationship with GSO and was the first local authority area in the UK to launch a Get Safe Online Digital Ambassador programme. The original programme had previously been delivered in a number of Commonwealth countries. WSCC took the programme and tailored it to work effectively at a local level. We have recruited and trained 23 volunteers, giving them key knowledge, tools and resources to deliver online safety advice and support. The Digital Ambassadors are now able to offer online safety advice and assistance via local communications, 1:1 session support with residents, local event attendance and delivering talks to community groups. The Digital Ambassadors in West Sussex have further developed our reach into communities identifying additional ways to share key digital safety advice. This has included working with a range of local parish magazines and writing blog posts to be shared via the County Council and other partners networks. As a result of the GSO programme and Digital Ambassador initiative, we currently have an estimated reach of around 200,000 residents receiving online safety information via various communications monthly. Further recruitment of more Digital Ambassadors is soon to start taking place. This to expand the network and to meet need where there are gaps of support coverage across the county.
- 1.38 Sussex Police lead a programme called Operation Signature. Operation Signature is the force campaign to identify and support vulnerable victims of fraud. As part of the initiative, if a bank has concerns about a customer's request, they can contact the police and 'freeze' the funds for 72 hours while officers attempt to engage with the individual and ascertain whether or not the transaction is fraudulent.

- 1.39 Sussex Police also lead on the delivery of the preventing victims of fraud programme. This programme links to the local training offer, events and resources delivered by WSCC.
- 1.40 The Southeast Regional Organised Crime Unit and WSCC have worked in partnership over the past 5 years to deliver a range of training and events to professionals, businesses and residents across the county. This has included training focused on young people being drawn into cybercrime, how businesses can prevent themselves falling victim to online crime and training for professionals about key cyber security principles. The SEROCU will soon be delivering training to Domestic Abuse professionals in relation to digital safety and online harm.
- 1.41 The County Council has been working with the NHS to support with digital safety as part of their Digital Inclusion agenda.
- 1.42 The County Council is part of Parent Zone's research partner network. Together the focus has been to improve how we can support and share key messages with parents and carers to support their children's digital resilience.
- 1.43 The district and borough councils' community safety partnerships support online safety messaging and events through their local networks and communities.
- 1.44 Chichester District Council and Arun District Council are looking to train their Community Wardens as GSO Digital Ambassadors to better incorporate digital safety as part of their roles.
- 1.45 The West Sussex Safeguarding Children's Partnership (WSSCP) are due to host a countywide safeguarding conference focusing on online risk and harm. Members of the County Council's Community Safety and Wellbeing Team (CSWB) will be presenting about key online risks and gamification. A stand will also be hosted during breaks to share information about the range of training and resources professionals can access.
- 1.46 The WSSCP have recently worked with CSWB to develop new webpage content to better inform digital safety information, training and resources. A number of children's services professionals have attended specific online safeguarding training sessions delivered by the CSWB Team on an annual basis. A recently launched online risk and harm training package is now available for children's safeguarding professionals to access. Training has also been delivered to foster carers and refugee families.
- 1.47 A range of training has been delivered to the County Council's Adult Service staff and Adult Safeguarding professionals. This has included scams awareness, online safeguarding, and specific subject matter areas such as romance fraud. The Prevention Assessment Team is very engaged with digital safety training and resources, they receive regular updates and communications about key online safeguarding issues.
- 1.48 The partnership also works closely with Neighbourhood Watch to promote and share the monthly GSO campaign material and other key online safety advice and resources with their large membership.

- 1.49 Information is regularly shared and presented to partnership groups including the Safeguarding Adults Board Children's Safeguarding Partnership and Prevent Board.
- 1.50 The SWSP is developing a new webpage to improve the way it can promote digital safety information and resources to its partners and communities.

Strategic Response

- 1.51 The County Council has committed to developing a cross-directorate digital access, inclusion and safety strategy that also has firm links across the wider statutory and voluntary sector partnership.
- 1.52 To do this we have identified an external partner, Citizens Online, with extensive experience in this field to review our approach and make recommendations on how the strategy can be delivered.
- 1.53 The strategy and any associated framework will further improve and support our partnership work to reduce online harm as well as improving how digital safety is embedded within digital inclusion and access delivery.

Service delivery in West Sussex

- 1.54 At the County Council, digital safety training, resources, and engagement activity for both professionals and residents are managed by the Digital Safety Lead Officer and delivered by the Digital Safety Delivery Officer, who work in the Community Safety and Wellbeing (CSWB) Team.
- 1.55 A range of training and resources are available for professionals and residents to access, produced and developed by the CSWB team. Training topics include online risk and harm, safeguarding adults and children online, gamification and online radicalisation, scams awareness, cyber security, cybercrime and romance scams. Resources include leaflets, guides, and a monthly staying safe online e-newsletter that has over 5,500 subscribers.
- 1.56 Due to the challenge of some County Council services and external partner organisations being able to attend in person training or live webinars, an online safety E-learning programme is being developed. This is currently scheduled to be available from April 2023 for staff and professionals working or engaging with adults/older residents.
- 1.57 The County Council's Countering Extremism Team offer and deliver training focussed specifically on gamification and extremism, delivering this across agencies. Both schools and wider professionals have accessed the training, which aims to increase awareness and build resilience to the risks associated with gaming and extremism.
- 1.58 A scheme of digital safety provision is being developed to support West Sussex refugees. On a fortnightly basis key safety information and guidance will be translated and shared with refugee families. This is in response to digital harm issues that the refugees have been experiencing.
- 1.59 Schools are required to meet online safety requirements as set out in 'Keeping Children Safe in Education' (September 2022). The Statutory guidance states that: 'All staff should receive appropriate safeguarding and

child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.' It is also recommended that schools consider any parental engagement.

- 1.60 Schools are also expected to meet online safety requirements as set out in RSHE guidance as well as the 2019 Department for Education guidance 'Teaching online safety in school'. The guidance states that the school culture should "incorporate the principles of online safety across all elements of school life ... Be reflected in the school's policies and practice ... And communicated with staff, students and parents." And "Schools should also ensure they extend support to parents, so they are able to incorporate the same principles of online safety at home."
- 1.61 In response to these requirements, the County Council developed a Digital Safety Package and associated training. This is available for schools to access help and enable them to support their pupils' digital resilience.
- 1.62 From September 2020, the new Relationships and Sex Education (RSE) curriculum became statutory in England. As part of RSE and Health education, online safety is considered a mandatory part of the teaching requirements for both primary and secondary schools.
- 1.63 In response to these new requirements, WSCC developed the Education for Safeguarding (E4S) curriculum. The E4S curriculum is based on the national Department for Education Relationships, Sex and Health Education (RSHE) guidance and numerous national frameworks, including the PSHE Association, but adapted and enriched for schools in West Sussex. It has been developed via a multi-agency approach combining teams from Safeguarding in Education, Contextual Safeguarding, Health and Education in West Sussex.
- 1.64 Digital and Media Literacy (DML) forms one of the four cornerstones of the E4S curriculum. The web resource overview pages that all schools can access, provide high level conceptual information about elements of digital and media literacy and links to guidance, training, and generic teaching resources. E4S subscribing schools can access more comprehensive information and quality assured resources mapped against the cornerstone concepts and themes. 65% of West Sussex schools are currently subscribed to E4S. Every school has free access April 2022 – April 2024.
- 1.65 The County Council's Library Service have embedded digital safety as part of the digital inclusion offer via training and associated resources. With online safety being a core element of digital inclusion, libraries have ensured all staff and appropriate volunteers are fully trained about the subject. All libraries offer Get Safe Online (GSO) leaflets that residents can collect, and key GSO resources and information are regularly shared via newsletters. Libraries offer residents digital skills support via the computer buddy volunteers and remote digital support service, staying safe online is always woven into the support offered. The service is currently delivering a device gifting project via referrals and have been supporting and enabling digital

safety events to take place at library venues. On average, around 1300/month digital support enquiries are answered by staff in libraries.

- 1.66 The County Council's Trading Standards team deliver a range of work and activity to support prevention of online harm including co-delivering scams awareness sessions for residents. These sessions have been in response to local fraud data. The data has shown that whilst there are still a range of 'traditional' fraud types that take place including door-step scams, there have been increased amounts of fraud taking place or being facilitated by digital technology. Having considered this, the WSCC Community Safety & Wellbeing Team together with Trading Standards now deliver joint awareness sessions which have been very well received by local communities.

2 Other options considered (and reasons for not proposing)

- 2.1 Not applicable as background report for information only.

3 Consultation, engagement and advice

- 3.1 Not applicable as background report for information only.

4 Risk implications and mitigations

- 4.1 Not applicable as background report for information only.

5 Policy alignment and compliance

- 5.1 Not applicable as background report for information only.

Emily King

Assistant Director (Communities)

Contact Officer: Francesca Blow, Digital Safety Lead Officer, 0330 2223851, Francesca.blow@westsussex.gov.uk

Appendices

Appendix 1: Statement from Jez Rogers, Southeast Regional Organised Crime Unit

Appendix 2: Statement from Swiss Gardens Primary School

Appendix 3: Statement from West Sussex Youth Cabinet

Appendix 4: Internet Watch Foundation research detail