# SURREY POLICE AND CRIME PANEL

## CyberSafe Surrey Project Update
## 1st December 2015

## 1. Summary

**1.1** To provide the Police and Crime Panel with an update on the work being undertaken as part of the CyberSafe Project.

### 1.2 RECOMMENDATIONS

1.3 Members of the Police and Crime Panel are asked to:

I. Note the content of this report;
II. Promote membership of the CyberSafe Network within their respective organisations.

### 1.4 EQUALITIES AND DIVERSITY IMPLICATIONS

1.5 No implications.

**LEAD OFFICER:** Damian Markland, Project Manager and Policy Lead for Cybercrime Prevention, OPCC

**TELEPHONE NUMBER:** 01483 639081

**E-MAIL:** damian.markland@surrey.pnn.police.uk

## 2 Background

**2.1** The development of the internet has radically altered the way in which we work, communicate, shop and interact. Recent data from the ONS indicates that 76% of adults in Great Britain access the internet every day and 74% use the internet to buy goods or services. At the same time, access to the internet using mobile phones more than doubled between 2010 and 2014, from 24% to 58%.

**2.2** This rise in use is particularly driven by young people. The 2013 annual report of the independent regulator and competition authority for the United Kingdom communications industries reported that 91 percent of children live in a household with internet access. In 2013, children aged 5-7 years spent, on average, 6.7 hours each week online; children aged 8-11 years, 9.2 hours; and children aged between 12 and 15 years, 17 hours.

**2.3** Whilst the internet has created numerous opportunities for both individuals and businesses, it has also provided new opportunities for criminals. Sometimes this takes the form of cyber-enabled crime, defined by the Home Office as traditional crimes which can be increased in their scale or reach by use of computers, computer networks or other forms of ICT. Examples include fraud, sexual offending, harassment and commercial damage. Conversely, cyber-dependent crime is defined as offences that can only be committed by using a computer, computer networks, or other forms of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks.

**2.4** There is growing national attention being placed on tackling cybercrime, but no one agency is responsible. Nationally, the NCA tackles serious criminality such as major fraud, service disruption activity and organised online child exploitation gangs. The South East Regional Organised Crime Unit (SEROCU) also has some cybercrime enforcement capabilities although lower value crime against business and individuals, as well as online bullying, stalking and harassment is down to local police forces to investigate. Action Fraud has also been set-up to centrally record online fraud and identity theft.

**2.5** With regards to preventative work, a number of national services have been launched over the last few years. Notable examples include the Government's 'Cyber Streetwise' programme, a public-private sector partnership known as 'Get Safe Online', and the Cyber-security Information Sharing Partnership (CiSP), a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

**2.6** Unfortunately, despite the significant resource put into cybercrime prevention initiatives, data suggests that national campaigns are struggling to drive behavioural change, with one third of Brits still failing on basic security measures[1] and many smaller businesses not adequately protecting themselves. Equally, our initial work with partners around cybercrime prevention revealed that we lack a shared understanding of what cybercrime means to Surrey, the risks are not well understood and cyber-safety advice and resources are extremely fragmented and of variable quality – making it hard for our local professionals and practitioners to know where to turn to for advice.

## 3. Project aims

**3.1** In light of the above, the purpose of the CyberSafe Surrey project has been to develop a robust and sustainable local approach to cybercrime prevention, one that compliments the Government's national agenda. The approach also acknowledges that cybercrime prevention is not simply a matter for the police, and that all agencies that work with our communities need to play a role.

**3.2** The project has four key aims. These are to:

i. Raise the profile and understanding of cybercrime in Surrey amongst partners.

ii. Ensure partners have access to the data and intelligence they need in order to determine appropriate local responses.

iii. Capitalise on the vast communication networks of partners to support targeted dissemination of preventative messages.

iv. Ensure coordination of preventative activity between partners in order to make best use of available resources.

## 4. Project objectives

**4.1** To support delivery of the above aims, the project includes the following objectives, which can be viewed as separate but linked strands of work:

[1] http://www.actionfraud.police.uk/news/one-third-of-brits-failing-on-basic-security-measures-jun15

8

### 4.1.1 Development of a CyberSafe Network:

**Status:** Launched 7 July 2015

**4.1.2** This is an online, collaborative resource for professionals and practitioners in Surrey, designed to empower them to better safeguard themselves and our communities from online threats.

**4.1.3** The Network is a key component of the project: providing a strong recognisable brand; ensuring partners have access to the latest alerts and advice, allowing targeted dissemination of preventative messages, supporting coordination and acting as a central resource hub for preventative material and intelligence.


*Fig.1 – CyberSafe Surrey Logo*

**Appendix 1** provides a more detailed overview of the Network's functionality and progress since its formal launch on 7 July 2015. We have also received some expressions of interest from other Force areas who are interested in developing their own Network, or developing the existing platform to make it a shared resource.

### 4.1.4 Development of a local Cybercrime Profile:

**Status:** Planned publication date March 2016

**4.1.5** Data concerning the level and extent of cybercrime in Surrey is fragmented, with many different local and national agencies holding key information. Data owners include Action Fraud, Trading Standards, Surrey Police, CISP, Home Office, Business Networks and local Councils.

**4.1.6** The project recognises that there is an urgent need to develop a shared understanding of what cybercrime means to Surrey, and this is being accomplished through the development of a local Cybercrime Profile that can be shared with partners (both directly and through mechanisms such as the County Single Strategic Assessment) to provide an evidence-base for the development of local priorities and strategies.

**4.1.7** Data will be collated from a number of sources, including the aforementioned agencies. The profiles will also make use of previous and planned survey data obtained by the Surrey Federation of Small Businesses and the Surrey Chambers of Commerce, plus data captured by Eagle Radio during their programme of work in Surrey schools around online safety.

**4.1.8** The above data will be complemented by primary research taking the form of a resident survey run by the OPCC, and with the assistance of the South East Regional Organised Crime Unit. The survey is being conducted on a regional basis in order to provide a greater sample size and within 72 hours has already had over 1,000 responses. We will continue to run the survey until February 2016.

**4.1.9** The final Cybercrime Profile document will be made available to partners through the CyberSafe Network and the proposed draft contents are provided in **Appendix 2.**

**4.1.10 Development of signposting hub:**

**Status:** Signposting Hub launched November 2015

**4.1.11** Direct outreach work with residents and businesses can be a powerful tool in raising awareness of cybercrime threats and educating individuals on preventative strategies. There exists a plethora of organisations that provide outreach services, although there has historically been little in the way of coordination and it has therefore often been difficult for local partners to identify the most appropriate provider for their needs. Further still, some partners have resorted to paying commercial providers for support, unaware that comparable free or subsidised services are available locally.

**4.1.12** To address these issues, the project aims to map existing local support services and develop a "Signposting Hub' where users can, at a glance, easily identify relevant providers. The Hub will be hosted on the CyberSafe Network and made available to both members and non-members.

**4.1.13** The OPCC is also working with organisations such as Get Safe Online, Cyber Champions and Eagle Radio to build upon existing support and provide a range of services that are 'free at the point of delivery' for partners. In instances where the OPCC is directly commissioning

8

services, outcomes will be carefully assessed to ensure good value for money.

**4.1.14 Engagement with existing Force projects:** There are a number of existing Force projects that touch upon some of the issues addressed by the CyberSafe project. Notable examples include Operation Signature (postal scams committed against the elderly), Operation Edisto (courier fraud) and work around Public Facing Digital Services. To ensure synchronisation with the CyberSafe project, the project manager has ensured representation on all relevant project boards.

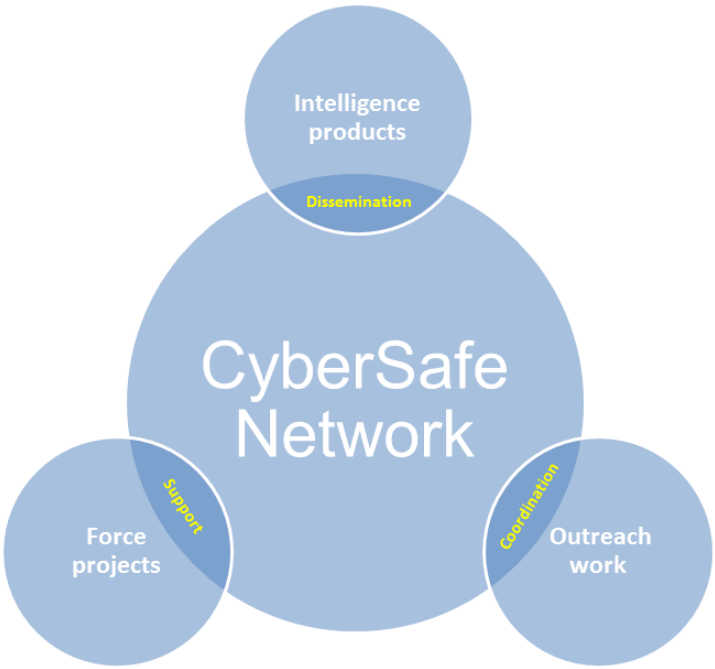


*Fig. 2: Visual representation of the project's key strands*

## 5. Project exclusions

**5.1** In accordance with the Police Reform and Social Responsibility Act 2011, the OPCC is not permitted to fetter the operational independence of the Chief Constable. In line with this, the CyberSafe Project has focussed exclusively on working with partners to improve Surrey's approach to cybercrime prevention and will not seek to influence operational policing.

## 6. Project deliverables

**6.1** To recap, the following products will be delivered through this project:

- An online collaborative platform to support cybercrime prevention in Surrey
- A Surrey Cybercrime Profile

- An agreed programme of outreach work and supporting signposting hub

## 7. Consultation and stakeholders

**7.1** Prior to commencement of the project, consultation was undertaken with the CyberSafe Group which consists of members from across the police, local councils, voluntary sector and private industry. Members were and have continued to be supportive of the work, and the Group now functions as a Steering Board for the project.

**7.2** Beyond the Steering Group, we have worked closely with a large number of local and national stakeholders, details of which can be found in **Appendix 3.**

## 8. Finance and Resources

**8.1** In the two years before the PCC took up office monies had been put aside by Surrey Police and Surrey Police Authority to fund the Surrey Drug and Alcohol Action Team (DAAT). The DAAT was responsible for commissioning treatment services for drug and alcohol in Surrey and was hosted by the Surrey Primary Care Trust (PCT). On closure of the PCT at the end of March 2013, the responsibilities for drug and alcohol abuse services passed to Public Health based at Surrey County Council.

**8.2** On the PCC's accounts for Surrey Police there is a balance sheet item of £430,000 entitled "The DAAT fund". In 2014/15 the PCC requested that internal audit carry out an audit of this sum of money to look at the funding of the DAAT and to seek to establish what should happen to the £430,000 which is contained within the balance sheet of the PCC and appears to relate to grant funding that was to be paid over to the DAAT. This audit did not find any clear partnership arrangement in place or owner for the funds. They therefore have remained unspent on the Surrey Police Group Balance Sheet.

**8.3** In light of the audit, it has been agreed that the PCC uses this money to fund activity aimed at reducing drug and alcohol misuse and cybercrime prevention work. This was reported to the PCP at its April 2015 meeting.

**8.4** Whilst there is sufficient funding to support two years of preventative work, a key objective of the team will be to ensure that the partnership model developed is financially sustainable in the long-term. It is felt that the development of the CyberSafe Network (see paragraph 3.1.1) will help ensure long-term sustainability beyond the lifetime of the project, as control can easily be transferred to or shared with another body.

## 9 Costs:

9.1 The following has been set aside to support the project in 2015/16.

| | | |
|---|---|---|
| **Staffing costs including associated on-costs** | Policy Lead<br>Policy Support | £85,000 |
| **Communications / Commissioning** | To support outreach work, research and development of relevant communication material. | £13,000 |
| **Set-up costs** | To support development of the CyberSafe Network* | £2,000 |
| | | **£100,000** |

* Please note, whilst this money was set aside to support development of the technical elements of the Network, this has so far been achieved using the in-house expertise of the OPCC, reducing costs.

## 10 Recommendations

10.1 Members of the Police and Crime Panel are asked to:

III. Note the content of this report;
IV. Promote membership of the CyberSafe Network within their respective organisations.