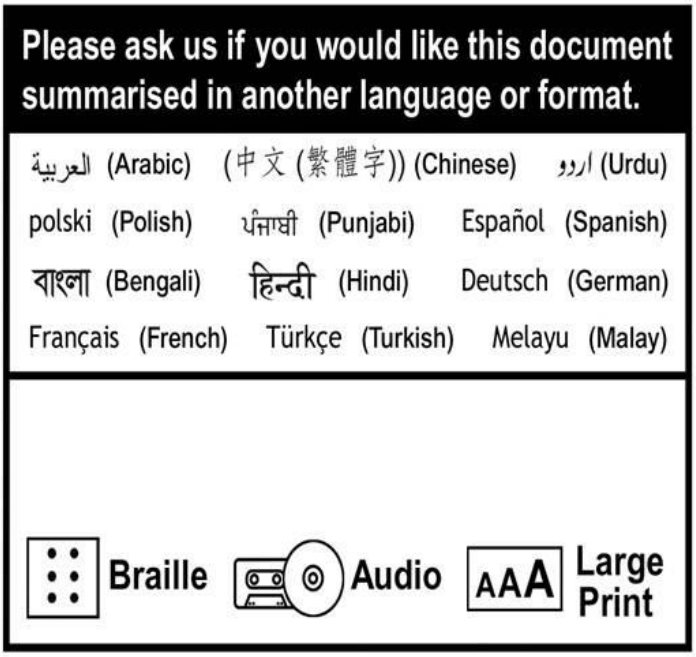

# Safer and Stronger Communities Overview and Scrutiny Report

# Cyber Crime

## 2018

# Contents





## Chair's Foreword

The internet can be fantastic for many young people to enjoy gaming, socialising and learning, but for what appears to be a minority it provides a platform to cause disruption and loss through forms of cybercrime including hacking which at times the offender may not fully understand the consequences of their actions.

In June 2017, Members of the Council's Safer and Stronger Communities Overview and Scrutiny Committee agreed to undertake review activity looking at work in relation to cybercrime. The focus of this work is on partnership work to prevent young people engaging in cybercrime activity.

At a national level, the National Crime Agency (NCA) is leading on a number of initiatives to prevent young people getting involved in cybercrime. Locally the Safe Durham Partnership's Cybercrime Task group together with the North East Regional Specialist Operations Unit (a collaboration between Northumbria, Durham and Cleveland forces to tackle serious and organised crime) are engaging with a wide range of people from school children to elderly people on prevention from being a victim. However, preventing vulnerable young people getting drawn into committing criminal activity was identified as a gap within their activity.

The committee agreed to undertake a review to gather initial research to support partnership work to gain an understanding of approaches to prevent young people becoming engaged in cybercrime activity. This work also provides an opportunity to raise awareness of this topic and identify any gaps or potential improvements.

We have gathered a wide range of evidence through desktop research, meetings with officers from the Council, partner agencies, the University of Sunderland, North East Regional Specialist Operations Unit and focus group sessions with young people.

The committee has a statutory responsibility for scrutinising the work of the Safe Durham Partnership and the findings in relation to education and awareness, career opportunities and campaigns have led to a number of recommendations for the partnership which also impact on the council.

I would like to take this opportunity to thank members of the working group and representatives from the Council's Partnerships Team and Children and Young People's Services, Durham Constabulary, North East Regional Specialist Operations Unit, Professor Irons, University of Sunderland and Durham Constabulary Police Cadets.

**Councillor Heather Liddle**
**Chairman**

## Executive Summary

1. At its meeting on 26th June 2017, Members of the Council's Safer and Stronger Communities Overview and Scrutiny Committee agreed to undertake review activity looking at work in relation to cybercrime.

2. Initially, the focus of this review is on partnership work being undertaken to prevent young people between the ages of 13-25 becoming engaged in cybercrime activity. However, from evidence presented at initial sessions this age range changed to focus activity on those aged between 10 -16 years old.

3. At a national level, the National Crime Agency (NCA) are leading on a number of initiatives to prevent young people getting involved in cybercrime. Locally the Safe Durham Partnership's Cybercrime Task group identified that locally, whilst work is very much active with victims of cybercrime, preventing young people becoming engaged in cybercrime was identified as a gap within their activity.

4. The aim of this review is to prevent young people within County Durham becoming engaged in cybercrime activity. Evidence and findings from this report are set within the context of preventing young people from becoming vulnerable and getting involved in cybercrime activity by seeking a more positive use of their skills. This is a developing area and the review provides an opportunity to raise awareness of this issue and seek to identify improvements to reduce the risk of young people becoming involved in Cybercrime. For full terms of reference and details of the meetings held during the review, **see Appendices 1 and 2.**

5. Evidence gathered throughout the review has highlighted the potential impact of cybercrime or a cyber attack and that this is not a victimless crime. The average age of suspects arrested or cautioned by the NCA for cybercrime is 17 years old. Whilst it was acknowledged that is a minority of young people who commit these offences, throughout the review anecdotal evidence was provided by Members, Officers and Police Cadets of awareness to incidents of hacking by young people.

6. It was highlighted that the motivations for undertaking this activity are not always financial. Some see it as a challenge and are unaware they are committing a criminal offence. In addition, offenders perceive the risk of being caught was low and there was a limited understanding of the consequences of the law and committing an offence.

7. There is a structured approach to tackling cybercrime and contributing to the delivery of the Government's National Cyber Security Strategy at a national, regional and local level. The review is also timely with consultation on priorities for the Safe Durham Partnership Plan. The Committee fully support cybercrime as an objective within the plan.

8. At a national level there is a wide range of educational resources and engagement activity available to schools. It is positive that within the past year, a small number of schools in the county have participated in the Cyber Security Challenge UK event. An area for development could be to have a co-ordinated approach to the use of educational resources and consideration should also be given to the development of a cyber-safety event and campaign in Durham.

9. Furthermore, effective provision of careers advice could lead to encouragement in using cyber skills more positively for career opportunities within cyber security industry. There was information provided that engagement between the Safe Durham Partnership and County Durham Economic Partnership had just begun with regard to cybersecurity apprenticeships within the County.

**Recommendations**

**Recommendation One -** That the Safe Durham Partnership Board note the content of this report and include as an action the prevention of people becoming cybercrime offenders within the Safe Durham Partnership Plan priority objective of Cybercrime.

**Recommendation Two** - That the Safe Durham Partnership Cybercrime task and finish group give consideration to holding further focus group sessions with Durham Constabulary's Police Cadets and with young people with a specific interest in coding or programming to improve young people's awareness to the Computer Misuse Act and its implications.

**Recommendation Three -** That the Safe Durham Partnership Cybercrime task group note findings of an anticipated report from the University of Bath, NCA and Research Autism into exploring any links between autism and cybercrime and consider any actions as recommended.

**Recommendation Four** - That the Children and Young People's Services note the availability of education and awareness resources and working with partners within the Safe Durham Partnership's Cybercrime task group consider development of a co-ordinated approach within schools to raise awareness to the consequences of forms of hacking, the Computer Misuse Act and use of careers advice to promote skills in a more positive way.

**Recommendation Five** - That the Safe Durham Partnership Cybercrime Task Group explore the feasibility of a cyber-safety engagement event with schools similar to the Partnership's Wisedrive/Safety Carousel event of which awareness to the consequences of the Computer Misuse Act and hacking is one of the workshops.

**Recommendation Six -** That the Safe Durham Partnership Cybercrime Task Group give consideration to undertaking a campaign to promote the risks of undertaking cybercrime activity and to explore the viability of producing a

video resource that could together with the NCA Cyberchoices videos be shown within schools and at events.

**Recommendation Seven -** That the Safe Durham Partnership explore opportunities for the development of IT/Cybersecurity apprenticeships within organisations and companies within County Durham with the County Durham Economic Partnership.

## Strategic Context

### *Key Findings*

- **2015 – There were 2.46 million cyber incidents and 2.11 million victims of cybercrime**
- **NCA report average age of 17 for cybercrime suspects**
- **Motivations are not always financial and offenders perceive the likelihood of encountering law enforcement as low**
- **Limited understanding of the impact of the Computer Misuse Act 1990**
- **Government's National Cyber Security Strategy published in 2016**
- **Structured approach to tackle cybercrime through national, regional and local resources**
- **Cybercrime is identified as a strategic priority for the Safe Durham Partnership Plan 2018-21**

**Background**

10. The National Crime Agency (NCA) estimates that the cost of cybercrime to the UK economy is billions of pounds per annum and growing. In October 2016, crime figures from Get Safe Online and Action Fraud revealed that £10.9 billion was lost to the UK economy as a result of fraud, including cybercrime, in 2015/16. The Office of National Statistics estimated that there were 2.46 million cyber incidents and 2.11 million victims of cybercrime in the UK in 2015. This is not a victimless crime and an attack can potentially cause devastation to those effected. Highly publicised cases include the TalkTalk security breach in 2015 and the WannaCry ransomware attack in 2017 that significantly affected a number of NHS Trusts.

11. Whilst the spectrum of types of cybercrime is wide, the focus of the Committee's work has been on activity by young people linked to types of hacking. The purpose for this approach is that analysis of investigations by the NCA's National Cyber Crime Unit reported that in 2015 the average of suspects was 17 years old. Information from Europol's website report the following examples of cybercrimes that involve predominately young offenders:

- ***Hacking*** - gaining access to a person's computer network without their permission and then taking control, and/or taking information from an organisation, agency or individual.

- ***Malicious software*** - making, supplying, or obtaining malware, viruses, spyware, botnets, and Remote Access Trojans (RATs) is a criminal activity. These programmes allow cybercriminals to get into other people's computers without their permission. "Pranking", by remotely accessing a friend's computer without their knowledge and messing around with it, is illegal.

- ***DDoS*** - a Distributed Denial of Service (DDoS) attack, or 'booting', consists of sending a large amount of internet traffic towards a website to stop somebody or anybody from accessing it.

12. The above are serious offences under the Computer Misuse Act 1990 but many young people who get involved in cybercrime do so for fun without realising the potential consequences of their actions. This is supported by findings within a NCA publication *'Pathways into Cybercrime'* that included:

    - 'Financial gain is not necessarily a priority for young offenders'
    - Completing the challenge, sense of accomplishment, proving oneself to peers is a key motivation for those involved in cyber criminality.
    - Offenders perceive the likelihood of encountering law enforcement as low.

13. This publication also stated that '*Autism Spectrum Disorder appears to be more prevalent amongst cyber criminals than the general populace though this remains unproven'.* To explore this further, a project is being undertaken by the NCA, University of Bath and the charity Research Autism to explore if there are any links between cybercrime and autism. It is requested that the Cybercrime Task Group note findings from this report.

14. The reality is that a young person who has been involved in cybercrime could receive a visit and warning from police or NCA officers, being arrested, a prison sentence of up to 10 years and or a criminal record that could affect education and future career prospects, as well as potential future overseas travel.

15. Evidence provided, highlighted that cybercrime through forms of hacking is underreported and is a barrier to understanding the complete picture as to the nature of these incidents, attempted attacks and who are victims and offenders.

16. To seek the views and gauge an understanding of the awareness on cybercrime by young people, a focus group session was held with Durham Constabulary's Police Cadets. Findings from this session showed that the impact on victims is not seen or understood by offenders, anyone could carry out a cybercrime attack or become a victim, many young people would do it to look cool and they would not be aware that they could receive a criminal record. Anecdotally, the group were aware of incidents of DDoS attacks and of peers who had the ability to 'hack' into systems. Further information from this session are referenced throughout the report but Members ask that consideration is given to working with the Cadets on cyber safety issues and for the partnership to hold a similar session with young people from school coding clubs.


17. There is a clear need to raise awareness of the potential consequences of young people unwittingly conducting criminal acts. The review initially planned for an age of 13 -25 but from findings from the NCA reports, an evidence session with the Council's Education Development Advisor and focus group sessions with police cadets, it is suggested that activity by the Safe Durham Partnership is targeted initially at the 10-16 age group.

***National and Local approaches to addressing the threat***

**Government Strategy**

18. The Government's 'National Cyber Security Strategy 2016-21' explains the Government's approach to tackling and managing cyber threats in our country. The strategy sets out how the UK will aim to be one of the most secure places in the world to do business in cyberspace and is written around the three objectives of Defend, Deter and Develop. The 'Develop' element of the strategy outlines the approach to growing an innovative cyber security industry and producing a sustainable supply of home grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence. It is within the context of encouraging young people to develop ICT skills for positive benefits and to have aspirations on entering the cyber security profession that this element of the national strategy is most pertinent to our review.

**National Cyber Security Centre (NCSC)**

19. The NCSC is part of GCHQ, the communications arm of the Government's intelligence community and was created in 2016 in support of a national ambition, outlined in the National Cyber Security to make the UK the safest place to live and do business online. The NCSC aims to help protect our

critical services from cyber-attacks, manage major incidents, and improve the underlying security of the UK communications infrastructure through technological improvement and advice to citizens and organisations. Within its '2017 annual review' it states that the '*cyber threat is real and growing and the types of threats we face are always evolving'*.

20. The NCSC promote information on their Cyber First programme for university students, apprenticeships and summer schools for teenagers. Furthermore, they are working with government departments to develop a skills programme for 14-18 year olds to embed cyber security as a recognised career choice.

***National Crime Agency (NCA)***

21. The role of the NCA is to protect the public from the most serious threats by disrupting and bringing to justice those serious and organised criminals who present the highest risk to the UK. The National Strategic Assessment of Serious and Organised Crime 2017 includes cybercrime as a threat and highlights underreporting of incidents as a barrier to gaining an understanding of its true scale and cost.

22. The NCA includes a National Cyber Crime Unit that leads the UK's response to the most serious of cybercrime threats. Preventing young people from getting involved in cybercrime is a key area of work for the NCA who through its website report what is cybercrime, its consequences, ways to use cyber skills more positively, career opportunities and advice for teachers and parents. These aspects are outlined within this report.

***Local Context***

23. A local perspective in tackling cybercrime is provided by the North East Regional Special Operations Unit (NERSOU), Durham Constabulary and other partners through the Safe Durham Partnership's Cybercrime Task Group.

24. NERSOU is one of 10 Regional Organised Crime Units across England and Wales, established in October 2013. It is a collaboration between the three forces of Northumbria, Cleveland and Durham. NERSOU includes a Regional Cyber Crime Unit (RCCU). At the time of the Committee's work, the cybercrime unit was being expanded through the recruitment of additional police officers.

25. The RCCU deals with the most serious pure cyber-dependent offences and high value cyber-related frauds.

26. The unit also works with police forces and the NCA to tackle serious and organised crime by providing investigative and technical support and a proactive cyber capability.

27. Within the county, Durham Constabulary has a dedicated Digital Intelligence and Investigation Team that comprises of specially trained detectives and police staff. The team will not only investigate digital crimes but will also

gather intelligence and stay up to date with the latest digital threats, viruses and scams.

28. The Safe Durham Partnership identified cyber-crime as an emerging threat in 2015 and set up a multi-agency Task and Finish group that includes representatives from NERSOU, Council, Fire Service, Police Crime and Victims Commissioner and Durham Constabulary to co-ordinate activities including raising awareness, education and how to tackle the threat.

29. At its meeting in October 2017, the Safer and Stronger Communities Overview and Scrutiny Committee received a report on findings from the Safe Durham Partnership's Strategic Assessment that identified cybercrime as a strategic priority for the Safe Durham partnership Plan 2018-21. Within its response the Committee suggested consideration to an action within this priority to include '*prevention of people becoming offenders'* of cybercrime.

**Recommendations**

***That the Safe Durham Partnership Board note the content of this report and include as an action the prevention of people becoming cybercrime offenders within the Safe Durham Partnership Plan priority objective of Cybercrime.***

***That the Safe Durham Partnership Cybercrime task group give consideration to holding further focus group sessions with Durham Constabulary's Police Cadets and with young people with a specific interest in coding or programming to improve young people's awareness to the Computer Misuse Act and its implications*.**

***That the Safe Durham Partnership Cybercrime task and finish group note findings of an anticipated report from the University of Bath, NCA and Research Autism into exploring any links between autism and cybercrime and consider any actions as recommended.***

## Prevention

### Key Findings

- **A wide range of educational and video resources available to raise awareness to consequences of hacking and cybercrime**
- **Cyber First and Cyber Security Challenge UK competitions encourage engagement from schools**
- **A Cyber Security Challenge UK event was held with Durham Schools in April 2017**
- **Young people should be encouraged to use cyber skills more positively for career opportunities within cyber security**

### Education & Awareness

30. This element of the report focuses on education and raising awareness to prevent young people becoming involved in cybercrime. This will focus on national and local perspectives to raise awareness of the Computer Misuse Act, highlight consequences of cybercrime but to also to promote how these skills can be used more positively including potential academic and career opportunities. A video outlining these risks by the NCA titled 'Cyberchoices' was presented to Members that highlight to parents the risks and help their children make the right choices.

31. At a national level and in line with the National Strategy, the NCSC lead the Cyber First programme that aims to deliver a range of activities designed to support talented young people through their education and highlight career opportunities in cyber security. The programme includes a number of residential and non-residential courses designed to introduce 11-17 year olds to the world of cyber security.

32. The NCSC webpage reports that females represent 10% of the cyber workforce and their programme includes a 'Cyber First Girls' competition for girls aged between 13 and 15. Their first competition in 2017 included over 8,000 participants within 2,171 teams from schools across the UK and its NCSC's hope that the event will help better represent women in the future cyber workforce. Furthermore, the cyber first programme includes a degree apprenticeship and the NCSC has certified Masters and Bachelor degrees in cyber security with a number of universities across the UK.

33. In November 2017, The Department for Digital, Culture, Media and Sport launched a cyber-security training programme called 'Cyber Discovery' aimed at young people in school years 10-13. The initiative aims to help plug the UK's cyber security skills gap by tapping into young and undiscovered talent with the ambition of stimulating and nurturing interest in cyber security as a future career path. In addition, the NCA's website promotes Cyber Security Challenge UK which is a series of national competitions, learning programmes, and networking initiatives designed to identify, inspire and enable more people to become cyber security professionals.

34. The above provides an outline to a wide and increasing range of education initiatives available to young people with an interest in cybercrime. Evidence provided, reported that within County Durham schools that elements of hacking were probably only considered by a small proportion of pupils and anecdotal examples were provided of where pupils who had initially been involved in gaming then became interested in hacking and required either police involvement. With regard to education, this is a developing area and work was very much active to raise awareness to cyberbullying, sharing of inappropriate images and staying safe online but there was no co-ordinated plan with regard to awareness and consequences of the Computer Misuse Act or hacking. Members were informed that in April 2017, six schools had taken part in a Cyber Security Challenge UK event within the county and this was an event to be explored again in the future. The Police cadets also indicated that whilst they were aware of incidents, they had limited knowledge of the consequences of hacking through the Computer Misuse Act.

35. To raise awareness, it is suggested that the Safe Durham Partnership consider development and collation of resources for schools for use with pupils aimed at 10- 16 years of age and ways and awareness to parents. This could potentially be undertaken through class assemblies or challenging programming tasks for a target audience that may divert any potential offenders to utilise skills more positively. In addition, messages could also be provided via partnership campaigns linking in with NERSOU and NCA utilising social media and video formats. These interventions were also identified within the NCA publication Identify, Intervene, Inspire – helping young people to pursue careers in cyber security, not cybercrime'.

36. Feedback from the Police Cadets highlighted the impact on young people short videos such as 'Kayleigh's Love Story' to raise awareness of online grooming and the 'Dying to be Cool' water safety campaign by the Safe Durham Partnership had. Reference was also made to the partnership approach to road safety using 'Wisedrive' and Safety Carousels and whether a bespoke event similar to this approach should be held on staying safe online. An element on the impact of hacking and awareness of the Computer Misuse Act could be included within this. Case studies may also be beneficial to highlight impact and there was a strong view from the Police Cadets that stark examples would be more effective when raising awareness on this issue.

**Apprenticeships & Careers**

37. As outlined there is a national drive to encourage more young people to enter the cyber security profession through educational courses including degree apprenticeships. The national cybercrime strategy states *'The UK needs to tackle the systemic issues at the heart of the cyber skills shortage*' to which includes a '*lack of young people entering the profession*' and '*shortage of current cyber security specialists'*. Whilst this approach is positive and can potentially lead to an exciting and rewarding career, Members emphasised the importance of apprentice opportunities being available within County Durham. A key challenge is to ensure that any opportunity is relevant for both

the young person and for the organisation. It was reported that this was an area to be explored by the Safe Durham Partnership together with the County Durham Economic Partnership.

**Prevention from remaining in cybercrime activity**

38. The 'Deter' element of the Government's National Cybersecurity Strategy includes a strategic outcome that 'the impact of cybercrime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK'. Within this outcome is a measurement of *'Improved effectiveness, and increased scale, of early intervention ("PREVENT") measures is dissuading and reforming offenders'*.

39. A key area to this work is prevention through education and awareness but also to the importance of understanding why young people become involved in cybercrime and to then identify deterrents and alternative ways to use their skills more positively. To gain an understanding of this issue, Members considered findings from a NCA report titled *'Identify, Intervene, Inspire – helping young people to pursue careers in cyber security, not cybercrime'*. The report provides detail on a potential pathway into cybercrime starting with gaming cheats and modifications with possible intervention points including ambassadors working in schools to identify people who could be at risk. The NCA has also produced two videos with reformed offenders. One video includes footage of a person speaking on the impact of receiving a custodial sentence for serious offences and the second video promotes changing routes and pursuing suitable career opportunities.

40. As part of its evidence NERSOU advised Members that in July 2017, Cyber Security Challenge UK working with the NCA held its first intervention workshop in Bristol with young offenders who had previously received cautions or cease and desist orders. Its aim was to prevent them from re-offending and to encourage them to consider ethical and legal jobs in the cyber security sector. This was a pilot event and the NCA aim to roll this out nationally as an on-going resource. Within County Durham, Members were informed that to date, neither the Checkpoint programme nor youth offending services have undertaken activity in relation to forms of cybercrime through hacking. It is within this context that this is a developing area and as part of an update on implementation of recommendations, the Committee should be kept appraised of the number of cease and desist visits that are undertaken within the County in relation to cybercrime.

**Recommendations**

- **That the Children and Young People's Services note the availability of education and awareness resources and working with partners within the Safe Durham Partnership's Cybercrime task group consider development of a co-ordinated approach within schools to raise awareness to the consequences of forms of hacking, the Computer Misuse Act and use of careers advice to promote skills in a more positive way.**

- **That the Safe Durham Partnership Cybercrime Task Group explore the feasibility of a cyber safety engagement event with schools similar to the Partnership's Wisedrive/Safety Carousel event of which awareness to the consequences of the Computer Misuse Act and hacking is one of the workshops.**

- **That the Safe Durham Partnership Cybercrime Task and Finish Group give consideration to undertaking a campaign to promote the risks of undertaking cybercrime activity and to explore the viability of producing a video resource that could together with the NCA Cyberchoices videos be shown within schools and at events.**

- **That the Safe Durham Partnership explore opportunities for the development of IT/Cybersecurity apprenticeships within organisations and companies within County Durham with the County Durham Economic Partnership.**

## Appendix 1

## Terms of Reference

The review has undertaken initial research to support partnership work to gain an understanding of approaches to prevent young people becoming engaged or remaining in cybercrime activity. This area was identified as a gap by the Safe Durham Partnership Cybercrime Task and Finish Group and to which the objectives of the review were:

- Linked to national and local objectives, the review will aim to gain an understanding of how young people can become engaged in cybercrime activity, why they are vulnerable and the risks and consequences of their engagement.

- To receive information on the approach and activity led by the National Crime Agency to prevent young people from engaging in cybercrime activity.

- To look at activity undertaken by the Safe Durham Partnership Task Group to raise awareness through education and engagement and how this links to the National Crime Agency's programme.

- To look at activity undertaken by the National Crime Agency, Regional Cybercrime Unit, Offender Management Unit and Youth Offending Service to prevent young people from remaining in cybercrime activity.

- To gather views of young people on cybercrime and possible methods to prevent young people becoming engaged in cybercrime.

# Appendix 2

## Review Meetings Held

The review has gathered evidence through desktop research, meetings with officers from the Safe Durham Partnership, Professor Irons, University of Sunderland, North East Regional Specialist Operations Unit and undertaken focus group activity.

| Date | Activity/Venue |
|---|---|
| 11/09/2017 | Working Group Meeting – Overview Session, County Hall, Durham |
| 16/10/2017 | Working Group Meeting – Prevention Education & Awareness from becoming involved in cybercrime – County Hall Durham |
| 14/11/2017 | Focus Group Session – Durham Constabulary Police Cadets – Police HQ, Durham |
| 17/11/2017 | Working Group Meeting – Prevention from remaining in Cybercrime activity, County Hall, Durham |
| 15/01/2018 | Working Group Meeting – Presentation of draft findings, County Hall, Durham |