|  |  |
| --- | --- |
| **Executive Board Minutes** | Logo  Description automatically generated |
| **Meeting Date:** *15th December 2022* |
| **Duration:** *09:00-11:00* |
| **Location:** *Dixon Room, Police HQ/Microsoft Teams* |

|  |  |  |
| --- | --- | --- |
| **Attendees** | | |
| **Durham Police and Crime Commissioner’s Office** | **Durham Constabulary** | |
| **Chair:** Joy Allen Police and Crime Commissioner (PCC) | Chief Constable: Jo Farrell | |
| Personal Assistant: Ashleigh White | Deputy Chief Constable (DCC): Ciaron Irvine | |
| Head of Private Office: Sweety Sahani (SS) | Assistant Chief Constable (ACC): Tonya Antonis | |
| Accountability and Scrutiny Officer: James Atkinson (JA) | Head of Governance and Insights: Sheena Urwin | |
| Policy and Accountability Officer: Kalim Askari | T/Ch. Supt Catherine Clarke | |
| Victims Champion: Michael Banks |  | |
| Head of Governance and Finance: Charles Oakley |  | |
|  |  | |
| **Apologies** | | |
| Assistant Chief Officer (ACO): Gary Ridley |  | |
| Policy, Commissioning and Accountability Lead: Jeanne Trotter |  | |
|  |  | |
|  |  | |
|  | | |
| 1. **Welcome and Introductions** | | **Action Owner** |
| PCC Mrs Joy Allen, as Chair, welcomed all members to the meeting.  Apologies were received as documented above.  There were no declarations of interest shared. | | PCC Joy Allen |
|  | |  |
| 1. **Minutes from the meetings held on 17th November 2022** | |  |
| Minutes from the previous Executive Board meeting held on 17th November 2022 were accepted and recorded as true record.  A copy of the minutes is available on the PCC website. | | Miss Ashleigh White |
|  | |  |
| 1. **PCC Action Log Update** | |  |
| All actions from the previous minutes have been completed and/ or progressed. | | PCC Joy Allen |
|  | |  |
| 1. **Thematic Report: Safer Online** | |  |
| ACC Tonya Antonis presented the Thematic Report on Safer Online to the Executive Board. Online and cyber-crime continues to be a growing area of policing. Digital policing has been a part of everyday policing for a significant amount of time. Upskilling the front line, alongside increasing capability and capacity within Durham Constabulary is a key feature within the force’s activity and future planning. There is a significant footprint around the digital world running throughout the organisation from ICT infrastructure, investigation, specialism, prevention, and victim support.  The number of cyber and fraud recorded offences continues to generally trend up compared to 2021, which in turn significantly expanded over 2020 compared to previous years due to the impact of Covid-19 and increased online activity throughout the world.  Cyber-crime affects people of all ages. However, most victims are of working age. Moreover, those aged 19-30 routinely make up the largest quantity of victims by age group. Therefore, the work of the prevention, protection, and prepare activity by the force, Regional Organised Crime Unit, and Business Resilience Centre is extremely important. A large amount of activity is conducted around schools and educational establishments as the impact on young people for this type of offending can be significant and long lasting, especially when offending involves child sexual exploitation.  Durham Constabulary has been engaging with the national Operation Soteria/ Bluestone project as one of the pilot police forces. This is a collaboration between academics and law enforcement to review and improve the policing response to rape and serious sexual offences. There are 6 pillars to this work, of which pillar 6 is digital. The research, findings, and year two theory of change plan and implementation are an ongoing body of work.  2023 will bring further investment into Durham’s digital response with the creation of further dedicated Digital Media Investigation posts. These posts will support Durham’s digital capability and capacity force-wide and ensure that the constabulary is ‘match-fit’ to proactively deal with emerging digital threats and investigations for years to come.  Over the course of the previous 18 months, a comprehensive review process has taken place over the force’s dedicated digital intelligence and investigation unit. The department is headed up by a dedicated Detective Inspector (DI). The DI also has responsible for economic crime due to the overlap between financial and cyber-crime. The force has a dedicated Online Child Abuse Investigation Team.  Partnership working with Social Services aims to identify children at risk at an early stage and ensure they are appropriately safeguarded at the earliest opportunity.  The primary prevent/protect/prepare activity will be focussed on targeted cyber scams around the shopping period from autumn and throughout the Christmas period.  Funding has been secured from the PCC to operate a Cyber Club for young people in County Durham and Darlington. This is currently in the process of match fund bidding from additional sources and will aim to offer a safe place for young people to learn cyber skills, coding, and promote Cyber Choices. There are ongoing educational initiatives delivered to schools and community groups around the risks of cybercrime and prevention opportunities. Since January 2022, over 900 school pupils, 500 higher education students, and over 1700 individuals have been reached via awareness sessions, victim care, and one-to-one advice. Over 350,000 people have been reached through social media engagement. Delivery of Internet Safety sessions within schools by cyber prevention officers and Child Exploitation and Online Protection (CEOP) trained PCSOs.  PCC Joy Allen thanked ACC Tonya Antonis for the comprehensive report on Safer Online and asked the following questions:   1. ***How can the force improve the way they use the National Fraud Intelligence Bureau monthly victim lists to identify and support vulnerable victims and others who require additional support?***   *Durham Constabulary is currently engaged in the NECVCU Level 1 service all non-vulnerable victims are contacted by NECVCU. Allowing Durham’s victim support to concentrate on more vulnerable cases.*  *Action Fraud (NECVCU) are constantly reviewing with the view to improving the services for victims, Durham police are engaging in these national initiatives to ensure victims within the force area are afforded the appropriate support and safeguarding, given the complexities associated frauds crime reporting and management.*  *Where vulnerability is identified, the Economic Crime Unit liaise with local NPTs and the Cyber Prevent Team to provide bespoke safeguarding and signpost for additional support.*   1. ***What success have the force had in pursuing and bringing to justice those who groom children online or those who download or share images of abuse and protect those at risk? And how can we improve current arrangements?***   *Durham Police have a specialist Online Child Abuse Investigation Team (OCAIT).*  *A national model is followed regarding the timeliness of initial action and safeguarding. As a force they comply with the relevant time limits, ensuring that the initial action is taken as early as possible, and suspects are brought to justice. Our performance in this area is rated as outstanding by HMIC.*  *The force also works proactively with ROCU’s across the country who proactively target those responsible for online grooming of children. Again, Durham is regarded nationally as one of the country’s top performing forces in this area.*   1. ***How are the force raising awareness alongside partners of how children and adults can stay safe online and how to recognise online grooming, exploitation, and radicalisation?***   *The Cyber Team are part of the Safer Cyber Working Group who collaborate with a range of partners including Schools, Durham County Council, County Durham & Darlington Fire & Rescue Service, Tenants Associations, Regional Economic Crime Co-Ordination Centre, VCAS.*  *A range of educational cyber programs have been developed covering cyber dependent and enabled crimes. The focus is to keep children and adults safe online.*  *Literature has been developed including ‘inclusive’ resources for those with learning difficulties so that they can live independently and be safe online. The Cyber Team work alongside several charities to raise awareness.*  *There are a range of resources available to the Cyber team and NPT officers/PCSOs. These have been produced by national charities and support children and adults in recognising online grooming and exploitation.*  *Local NPT Officers/PCSOs work alongside schools and partners in their area to facilitate delivery and the Cyber Team & NPTs work alongside partners including AAPs/community partnerships/Cllrs to set up ‘roadshows’, covering various themes including cyber safety.*   1. ***How much has the force invested over the past year in improving digital investigation and intelligence to combat internet cyber enabled and cyber dependent crime? And what are the future investment plans in this space?***   *During 2022 the force restructured, aligning the Cyber Prevention team with the wider prevention arm of the organisation to increase exposure across prevention and partnership. The Cyber Pursue team remain aligned with investigation and are now within the same hub as Economic Crime due to the crossover in the fraud arena.*  *The force has invested in a dedicated Sergeant in the Digital Forensics Unit, to drive performance and safeguard future capability and capacity in this area.*  *The force has increased open-source capability and training users throughout the force area, specifically around areas which utilise large volumes of online investigation and intelligence.*   1. ***How does the force assess the impact and effectiveness of specialist roles such as the Cyber Prevention Officers?***   *Performance is monitored in Force through the Prevention & Problem-Solving Team.*  *Data captured includes.*   * 1. *Social media reaches – Number people who have seen post.*   2. *Social media engagements - Number of reactions, comments, shares and clicks on a post.*   3. *Number of events and audience – Including Businesses, schools, charities, youth clubs, community groups.*  1. ***What is the force doing to encourage all victims of cybercrime and online fraud to report, given that it is likely many digital crimes go underreported?***   *Durham Constabulary has a Media strategy relating to reporting of crimes to Action Fraud. There is specific signposting to Action Fraud on Durham Constabulary website and education packages have slides dedicated to ‘reporting’ including how to report and why it is important. Training is given to all Police Officers/PCSOs relating to reporting. ‘Keep in the Know’ messaging sent relating to online fraud and reporting.*   1. ***What is the turnaround time in processing digital devices linked to low and medium risk cases (particularly those linked to child exploitation and online protection type cases) and how does this impact on the force’s capability to identify potential victims and suspects in those ‘lower risk’ cases?***   *The Digital Forensics Unit (DFU) has a strict risk assessment process in place, utilising both THRIVE and KIRAT (Kent Internet Risk Assessment Tool) to ensure risk is understood, assessed, and mitigated to ensure all ongoing risk to children is minimised. A holistic approach is taken, factoring in the wider investigation and not simply the submission of the devices.*  *All cases to DFU are triaged by a technician prior to full forensic examination, creating a staged approach and ensuring timely identification of any unknown risk.*   1. ***It is noted that there is a significant rise in child suspects linked to the sharing of indecent images of children, what pro-active action is being taken locally to tackle this?***   *Where possible, all CEOP investigations involving child suspects are dealt with by the specialist OCAIT.*  *All the force’s NPTs and the Cyber Prevention team deliver inputs to children in education alongside the inputs the education sector delivers themselves.*   1. ***What measures does the force have in place to minimise the impact on victims from the examination of their digital devices?***   *Over 500 officers are trained in mobile phone extraction, thus enabling a timely response.*  *Victim mobile phones are almost always returned within 24hrs, and the force provides data to the Home Office in relation to the performance around this.*  *Data Processing Notices are completed with the victim for every device that the police take with consent. This has agreed extraction parameters and must be authorised by an Inspector, minimising any invasion of privacy.*   1. ***Given the force has invested in capacity in terms of both a proactive and reactive response to a range of cyber related offending, does the force have any indication around of the levels of repeat victimisation?***   *The Cyber teams receive a weekly list of victims who have reported to Action Fraud is disseminated to the team. The ROCU highlight any repeat victims.*  ***Less than 1%*** *are repeat victims. All victims receive an enhanced service. All victims who are identified as vulnerable will be subject of a safeguarding report which is shared with partners in the MASH.*   1. ***What impact does the force envisage coming from the new legislation currently going through Parliament in relation to online harm?***   *The Online Safety Bill has changed several times and it is difficult to give a definitive answer until the legislation has been agreed. The primary onus is on Internet Service Providers to remove harmful content and protecting users from this content. This will likely increase reporting to police, which will likely result in further police demand on the frontline, on investigators and on Digital Forensic Units. However, most large platforms already have established reporting mechanisms to police resulting in CEOP referrals to forces.*  *The bill also looks to further preserve and enhance freedom of speech, reinforced by recent case law.*  *New proposed offences under the bill at this stage would currently be already recorded as crimes and investigated as Malicious Communications.*   1. ***How is the force evaluating the effectiveness of fraud protection advice given to the public?***   *The force has introduced a fraud dashboard which has allowed a better understanding of the fraud landscape within the force area. This will also allow for bespoke protection advice to be provided as trends are identified.*  *Durham continues to support the national fraud prevention campaigns that take a thematic approach. Online fraud is ordinarily reported to Action Fraud.*  *Calls for service are attended by frontline officers who would investigate, safeguard, and provide appropriate victim advice & care, signposting to victim support.*  *The Durham Constabulary website provides advice & guidance in relation to fraud and where to appropriately report* | | ACC Tonya Antonis |
|  | |  |
| 1. **PCC Accountability Report** | |  |
| Mr J Atkinson presented the Accountability Report to the board; There were 44 items of correspondence received by the PCC’s Office in November 2022; this is an increase of 47% in correspondence compared to October 2022 (30). Most correspondence was classified as either an Expression of Dissatisfaction (17) or External Signposting (8). Service Behaviour (5) continued to place in the top two most common categories on the Caseworker system during November. These included items such as claims of wrongful arrest, report of racism, and dissatisfaction with lack of communication.  With regards to scrutiny, four separate external scrutiny panels (Rape, Domestic Abuse, Complaints, Police Powers) have independently raised concerns around Body Worn Video Footage. The concerns comprised of its absence, poor quality, and premature ending. The OPCC are working closely with the SCORD department to monitor the progress in this space. There has been investment for new cameras and a youth scrutiny group is going to be set up in due course.  There has been a commitment by the force (using precept investment) to invest in additional call handlers and digital solutions in the Force Control Room. Notwithstanding, the recent national data pertaining to 101/999 call data is set for further consideration and is cause for some solicitude. This is held within the context of increased demand, capacity to deal in terms of staffing, and issues with external service providers involved in call handling. It is positive to see the live chat function moving to a 24/7 service, the impact of which will be awaited.  Item to note- The thematic, data package, and public meeting programme of work is detailed in Appendix 2 for final Executive approval. The themes have been timed to best reflect the national and local policing calendars. A forward plan will be shared with the force upon development.  ***Good News Stories:***  Durham is highlighted as an example of best practice in the recent APCC national publication ‘PCCs Making a Difference: Victims in Focus’ in three key areas; advocating for victims, developing innovative services for victims and for using multi-year funding to fund quality services for victims.  It has been positively reported on by HMICFRS and the PCC that Neighbourhood Crime fell by 23.5 per cent in the first two quarters of 2022/23 when compared with pre-Covid rates in 2019/20. In addition, the rate of Neighbourhood Crimes that were successfully resolved climbed by four per cent to 15.9%.  The VCAS and Community Peer Mentors now have their own dedicated websites which will augment signposting to the services respectively.  A new Chief of Staff has been appointed to the OPCC after the formal confirmation hearing at the Police and Crime Panel. | | Mr James Atkinson |
|  | |  |
| 1. **Digital Data and Technology – Bi-annual Update** | |  |
| Temporary Chief Superintendent Catherine Clarke presented the Digital Data and Technology (DDAT) Bi-annual update. We have taken learning from recent national cyber incidents affecting Policing to improve our own position in Durham. We have implemented a Cyber Incident Response Plan and a new enhanced Incident Management Process within ICT, which has been rolled out to all teams aligned with the new DDAT Kanban operating model. There is an improved Privileged Identity Management (PIM) Process for out of hours security incidents to improve on-call staff access to what they might need to monitor, identify, and respond to in terms of cyber security concerns. This ensures auditability but removes single points of failure. Durham’s Skills Matrix is evolving and is more detailed considering the standard set of required skills to support the Estate whilst evolving Cyber related skills to ensure there is the capability to deliver, albeit capacity is still an issue and is a work in progress.  **EE Mobile Coverage**  The improved EE Mobile Coverage was completed in HQ.  The performance of the 4G signal has been excellent since completion which allows us to have improved communications and an extra level of resilience when running a Command Room or needing to urgently contact a member of staff, also for business-as-usual connectivity requirements.  **Red Sigma**  In October, Red Sigma was updated to include Victim Care changes required to deliver the needs of both the Victims Code and Bill and to enable the service to victims to be improved through better information gathering and exchange.  After an exploration of the UK Records Management System (RMS) market, Durham have discounted any of the current offerings and will continue to upgrade and develop Red Sigma as the main RMS system and have set out an ambitious 3-year plan.  The appointment of a Red Sigma Project Manager will allow more control and direction in relation to the next steps.  **Operation London Bridge**  ICT Engineers provided a mobile solution for the uploading and charging of BWV Cameras for officers deployed to Op London Bridge. Business Change staff attended the briefing and issued the requisite equipment to staff. We also ensured that a short notice high importance change was deployed to officers’ Airwaves radios to ensure the network could be used at maximum capacity.  **New Operating Model**  There is a new Operating Model for DDaT to ensure a single-entry point into the command for work requests and incidents requiring DDaT support. This will ensure all service requests are logged and tracked to remove direct approaches to staff which could cause a delay to ongoing priority work. This will allow us to ensure we manage the business outcomes required to deliver a continuously improved value service via a well-defined and communicated operating model.  **Information Management Training**  Staff across the Information Management, Business Change, and Information Rights & Disclosure Unit (IRDU) teams have either completed or are booked to attend specialist training supplied by the NPCC in Data Protection Fundamentals, Subject Access, Data Protection Impact Assessments, and Information Sharing Agreements. This will enhance cross-departmental understanding of Data Protection, which is now embedded from the outset of projects as part of the new DDaT Operating Model.  **Information Management**  Representatives for Durham sit on the National Data Sharing Quality Assurance Panel and were instrumental in identifying that the Data Protection Impact Assessment (DPIA) for the NIAM and NLEDS systems proposed by the Home Office and NPCC were not fit for a policing purpose and subsequently led the work to improve and complete them.  Durham Constabulary are in the process of recruiting a Chief Data Officer to lead Data Strategy. | | T Ch Supt Catherine Clarke |
|  | |  |
| 1. **Any Other Business** | |  |
| There was not any other business raised at this meeting. | | PCC Joy Allen |
| *Next Executive Board Meeting: Thursday 26th January 2023* | |  |