Opening Statement of An Garda Síochána to Joint Committee on Children and Youth Affairs
Wednesday, 25th October 2017, at 9.30am.

‘Cyber Security for Children and Young Adults’

The Garda Síochána’s Modernisation and Renewal Programme 2016-2021 represents the first time the organisation has laid out its mission, direction, plans and challenges spanning a five year period.

The fact that criminal activity changes and extends into new areas at a pace and that we have to react quickly and flexibly to cope with developments, is stated in the document. In this regard, the Garda Síochána has recently made major changes in response to organised crime and security threats, and has new strategies to address other emerging crimes and security challenges.

In particular online child sexual exploitation is a constantly evolving phenomenon and is shaped by developments in technology, mobile connectivity, growing internet coverage in developing countries and the development of pay-as-you-go streaming solutions, which provide a high degree of anonymity to the viewer and are furthering the trend in commercial live-streaming of child sexual abuse. Thus, it is necessary for the Garda Síochána to ensure it enhances its capacity to tackle the criminality involved, while being particularly alert to the vulnerability of its potential victims.

To a significant extent, responsibility for personal online security and protection rests with the user. However, as users get younger and are not as likely to be alert to cybercrime, especially in circumstances where the age of digital consent is to be lowered to 13 years, personal responsibility must also be supported by parents, teachers and responsible entities including State agencies such as the Garda Síochána.

The issues surrounding unrestricted access to Wifi are well publicised. Controls which existed at an earlier time in circumstances where children accessed the Internet at home or elsewhere under some form of supervision, have been eroded by the prevalence of internet cafes and mobile technology. It is now possible that a very young child can use a mobile phone to access the Internet over available public Wifi networks and can search for or come upon pornographic or violent material with little or no parental control.

Increasingly children are engaging in the sharing of self-taken imagery where they send nude and/or sexually explicit personal photographs of each other, to other members of a chat group, utilising platforms such as WhatsApp or Instagram, or over social media such as Facebook or Snapchat. While this scenario has given rise to a form of bullying, there is an added danger when images are circulated outside the confines of friends or otherwise become available to third parties, who may then use them as a trap to engage with a child or set up ‘fake profiles’, using the images as bait.

The Modernisation and Renewal Programme sets out clearly that victims of crime will be put at the heart of the service provided by the Garda Síochána. In this regard, in 2015, the Garda Síochána established twenty-eight Victim Service Offices across the country which are tasked with communicating with victims of crime and prioritising their needs. Protective Services Units (PSUS) which will operate within each Garda Síochána division will assist in ensuring that relevant child protection, domestic and sexual violence incidents are thoroughly investigated and victims fully supported.
In 2015, through the creation of the Garda National Protective Services Bureau (GNPSB), a number of units operating in various locations throughout the Garda Síochána, were brought together to leverage their experience and expertise in investigating serious crimes against vulnerable people. The GNPSB is a specialist team dedicated to making sure each and every complaint relating to child protection, human trafficking and domestic and sexual violence is thoroughly investigated and that such investigations are handled in an appropriate manner. In addition, GNPSB is responsible for working with other agencies to manage sex offenders in the interest of community safety.

Among the specialist units now located within the Garda National Protective Services Bureau (GNPSB), are:

(i) Sex Crime Management Unit;
(ii) Online Child Exploitation Unit;
(iii) National Child Protection;
(iv) Sex Offender Management and Intelligence Unit;
(v) National SORAM office. (Multi agency office staffed by a member of GNPSB, the Probation Service, the Child and Family agency (TUSLA) and a representative from Dublin City Council housing section to manage sex offenders);
(vi) Human Trafficking Investigation and Co-ordination Unit;
(vii) National Victims Office and Missing Persons Unit

Within the Online Child Exploitation Unit at the Garda National Protective Services Bureau (GNPSB) a new unit has been created which is tasked with the identification of online victims of exploitation.

Personnel attached to the Garda National Protective Services Bureau (GNPSB) have received training to enable them to perform the role of specialist victim interviewers.

Members of the Garda Síochána are often the first people victims of crime make contact with after a crime has been committed. Victims of crime will often have experienced a traumatic and potentially life-changing experience and may be vulnerable and require help and support. However, while getting the first contact with a victim right is critical, so too is ensuring this care and attention continues as their case, which is incredibly important and personal to them, moves through the justice system.

The Garda Síochána is acutely aware of the emotional and physical suffering of victims of child abuse and the fact that their experience may make it very difficult for them to report the crimes they have suffered. They may also feel that their complaint will not be taken seriously or fully investigated.
The Online Child Exploitation Unit (OCEU) at the Garda National Protective Services Bureau has responsibility for the enforcement of the provisions of the Child Trafficking and Pornography Acts 1998 to 2004, the investigation and co-ordination of cases relating to the possession, distribution and production of child pornography and any related sexual abuse of children. The unit is responsible, also, for the proactive investigation of intelligence concerning paedophiles and their use of technology and the online targeting of suspects for the production, distribution, and possession of child abuse images on the internet.

New strategies have been developed to meet the ever increasing challenges of cyber security and cyber crime. The Modernisation and Renewal Programme sets out the intention of the Garda Síochána to expand our capabilities with regard to cyber crime, through training with academic partners, increased investment in technology and people, and regionalisation of the investigation of computer crime, which for many years was located within the Garda National Economic Crime Bureau (GNECB).

The Garda Síochána will establish a new National Cyber Security Desk (NCSD) located at Crime and Security. It will liaise with national and international stakeholders including the Europol National Unit (ENU), Interpol National Central Bureau (NCB), police partners and security organisations such as Europol (EC3), the European Network and Information Security Agency (ENISA), and Interpol.

It is also planned to establish a Telecommunications and Information Technology Security Operations Centre. This Centre will include two separate dedicated units to deal with anomalies in Information Systems Networks and provide cyber and forensic tools and infrastructure to support operational policing and State Security activities.

The Garda National Cyber Crime Bureau (GNCCB) was established in September 2016, providing an enhanced structure within the Garda Síochána for the purpose of tackling cyber crime. The Bureau has a national remit with regard to the phenomenon of cyber crime and in particular the investigation of online criminality. The GNCCB is tasked with undertaking the forensic examination of computer media in all incidents reported to the Garda Síochána. Furthermore, this Bureau is given a role with regard to the provision of crime prevention advice to the public and the corporate sector regarding online offending and e-safety. This includes the provision of Internet safety advice.

Regional Cyber Crime Investigation Units (CCIU) are being established and regional units are currently operating successfully, on a pilot basis, in New Ross, Co. Wexford and Ballincollig, Co. Cork. The regional CCIU units will provide computer forensic services locally, under the supervision of the Garda National Cyber Crime Bureau (GNCCB). With a view to further supporting the regional units, it is planned to develop and roll-out first responder and triage capability nationally. These first responders will support the regional units and provide for a tiered level of capability nationally with the GNCCB as the top tier of support and capability.

The Garda National Cyber Crime Bureau (GNCCB) in conjunction with the Garda College has developed a training module relating to the investigation of cyber crime for delivery to all students attending the College. It is planned that other members of the Garda Síochána will be trained in cyber crime awareness and cyber crime investigation, through our Continuous Professional Development (CPD) network.
The Garda Síochána will further its long standing relationship with the Centre for Cyber Crime Investigation in University College Dublin through the CCIU and alumni who have undertaken courses of study at the University in the cyber domain. The Garda Síochána will also develop more educational partnerships with third level institutions and international institutions with expertise in cyber security in order to ensure cutting-edge knowledge is available throughout the organisation. We will look for opportunities to further develop relationships and share expertise.

In November 2017, personnel attached to the Garda National Cyber Crime Bureau (GNCCB) will travel to Lyon, France to participate in Specialist Victim Identification Training relating to Crimes Against Children, which is being delivered by Interpol. This course will address the issue of the vulnerability of children arising from the availability of child exploitative material on the internet.

Any individual, adult or child, business or organisation using a connected device is vulnerable to cyber crime. Just as with offline crime, simple steps can often be effective in reducing these vulnerabilities. Working in partnership with public and private sector stakeholders, CCIU will use opportunities such as the Garda Síochána’s communication channels, Crimecall, and public awareness campaigns to ensure people are educated on protecting themselves from cyber crime. We will further develop our crime prevention activities in this area.

While it is not feasible to regulate or monitor the internet in anticipation of all possible incidents such as cyber bullying, if a member of the public becomes aware of activity on the internet which they suspect may be illegal, they can report it confidentially to Hotline.ie which is operated by the Internet Service Providers Association of Ireland with oversight by the Office for Internet Safety (OIS) in the Department of Justice & Equality. Hotline.ie provides the public with the means to report illegal online content, such as child sexual abuse material and liaises with the Garda Síochána, as appropriate, to have illegal content taken down.

The Office for Internet Safety (OIS) is responsible for developing strategic actions to promote the highest possible levels of internet safety, particularly in relation to combating child pornography.

A dedicated website www.internetsafety.ie is supported by the OIS and provides information and links to other resources on internet safety. In addition, it partners with experts to develop and publish a series of information booklets on internet safety which are made available on the website and also in hard copy.

In November 2014, the Garda Síochána launched an initiative on the blocking of child sexual abuse material (CSAM) on the internet in Ireland. The OIS has an oversight role in the operation of Hotline.ie and the Garda Síochána blocking initiative. Hotline.ie is the confidential service for reporting illegal content in the internet in Ireland and it liaises closely with the Garda Síochána in carrying out its functions.

In November 2017, personnel attached to the Garda National Cyber Crime Bureau (GNCCB) will travel to Lyon, France to participate in Specialist Victim Identification Training relating to Crimes Against Children, which is being delivered by Interpol. This course will address the issue of the vulnerability of children arising from the availability of child exploitative material on the internet.

Any individual, adult or child, business or organisation using a connected device is vulnerable to cyber crime. Just as with offline crime, simple steps can often be effective in reducing these vulnerabilities. Working in partnership with public and private sector stakeholders, CCIU will use opportunities such as the Garda Síochána’s communication channels, Crimecall, and public awareness campaigns to ensure people are educated on protecting themselves from cyber crime. We will further develop our crime prevention activities in this area.

While it is not feasible to regulate or monitor the internet in anticipation of all possible incidents such as cyber bullying, if a member of the public becomes aware of activity on the internet which they suspect may be illegal, they can report it confidentially to Hotline.ie which is operated by the Internet Service Providers Association of Ireland with oversight by the Office for Internet Safety (OIS) in the Department of Justice & Equality. Hotline.ie provides the public with the means to report illegal online content, such as child sexual abuse material and liaises with the Garda Síochána, as appropriate, to have illegal content taken down.

The Office for Internet Safety (OIS) is responsible for developing strategic actions to promote the highest possible levels of internet safety, particularly in relation to combating child pornography.

A dedicated website www.internetsafety.ie is supported by the OIS and provides information and links to other resources on internet safety. In addition, it partners with experts to develop and publish a series of information booklets on internet safety which are made available on the website and also in hard copy.

In November 2014, the Garda Síochána launched an initiative on the blocking of child sexual abuse material (CSAM) on the internet in Ireland. The OIS has an oversight role in the operation of Hotline.ie and the Garda Síochána blocking initiative. Hotline.ie is the confidential service for reporting illegal content in the internet in Ireland and it liaises closely with the Garda Síochána in carrying out its functions.
The Garda Síochána signed a Memorandum of Understanding (MOU) with a large internet service provider under which the service provider agreed to block access to CSAM based on information which we provide to them. The Garda Síochána continues to engage with other service providers with a view to establishing further MOUs.

The Garda Síochána provides crime prevention advice to the public and the corporate section regarding online offending and e-safety. This includes the provision of Internet safety advice to schools, third level institutions, through the Campus Watch programme, the public, through media releases, such as the recent ‘Malware Awareness’ Campaign and regular information releases in the national publications and the Crimecall programme.

Section 3 of the Communication (Retention of Data) Act 2011, obliges Internet Service Providers (ISPs) to retain data for one year, however there is no penalty for a failure to retain such data. Section 7 of that Act requires ISPs to comply with a disclosure request made by the Garda Síochána pursuant to section 6 of the said Act. However, if internet providers fail to provide the Garda Síochána with data pursuant to the Communication (Retention of Data) Act 2011, our ability to identify people involved in the sexual exploitation of children or the distribution of child pornography on the internet, will be restricted.

The investigation of all the relevant incidents and the examination of associated computer media is dependent on the disclosure of a criminal offence. In cases involving the online safety of our young people the primary offences are cyber bullying and sexual exploitation. In this regard, the relevant legislative provisions are contained in the Non Fatal Offences Against the Person Act 1997, the Child Trafficking and Pornography Act 1998 and the Criminal Law (Sexual Offences) Act 2017.

‘Lockers’ is a new information and education resource designed, in conjunction with the Garda Síochána, to assists schools in coping with and preventing the sharing of explicit self-generated images of minors. Intended for use within the Junior Cycle Social Personal and Health Education (SPHE) curriculum, ‘Lockers’ is supported by a newly developed animation and six lesson plans and includes an information section for school leaders. This 25-page section informs principals on the context for ‘sexting’ among young people, the laws that can come into effect when underage sexting occurs and the implications for school policy.

The Garda Síochána is currently involved in the development of a new Webwise campaign, provisionally entitled ‘Exposed’, for delivery through secondary schools as a follow-on from ‘Lockers’. This new campaign will be designed to address the issue of the sexual exploitation of children through the use of technology and will incorporate the Say No! campaign launched earlier this year by Europol with the support of the Garda Síochána. The Say No! Campaign including a 10-minute video clip was launched to advise the public on ‘sextortion’, the threatened release of self-generated sexual images or information to extort money or to coerce a person to provide more images, engage in sexual activity, or to do something they otherwise would not do.

In 2010, the European Union (EU) set up a four-year policy cycle in order to create a greater measure of continuity for the fight against serious international and organised crime. The policy calls for effective cooperation among:
- law enforcement agencies,
- other EU agencies,
- EU institutions,
- relevant third parties.

The EU initiative gave rise to the European multidisciplinary platform against criminal threats (EMPACT). Europol has identified nine (9) priority crime areas. For each one, a multi-annual strategic plan, an EMPACT project and an operational action plan (OAP) are implemented. As a form of cybercrime, child sexual exploitation is one of the nine EMPACT priorities, Europol’s priority crime areas, under the 2013-2017 EU Policy.

Europol’s European Cybercrime Centre (EC3) supports the competent authorities in Member States in preventing and detecting all forms of criminality associated with the sexual exploitation of children.

It provides assistance and expertise in combating the distribution of child abuse material through all kinds of online environments, and tackles all forms of criminal online behaviour against children, such as grooming, self-generated indecent material, sexual extortion and live-streaming on the web.

Fighting the distribution of child abuse material includes preventing and intercepting it, and stopping it from being shared through peer-to-peer networks, as well as through commercial platforms. In this regard, EC3 is involved in the European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC), a network funded by the European Commission composed of law enforcement, NGOs and public and private sector stakeholders.

EC3 is also involved in the Virtual Global Taskforce (VGT), a collaborative partnership of law enforcement agencies, who have come together across the digital divide to combat online child sexual abuse worldwide. The Report abuse button on the VGT website is an effective way to report suspicious online behaviour.

Cooperation at an international level has proven to be very effective in identifying victims of child sexual abuse and exploitation. In 2015 Europol hosted a Victim Identification Taskforce, which resulted in 240 new collections of material being uploaded to Interpol’s child sexual exploitation image database and the extension of the existing 100 collections.

In addition, Europol’s Project HAVEN (Halting Europeans Abusing Victims in Every Nation) supports EU Member States in detecting and intercepting child sexual offenders travelling abroad to abuse children.

The Violent Crimes Against Children International Task Force (VCACITF) is a select cadre of international law enforcement experts working together to formulate and deliver a dynamic global response to crimes against children through the establishment and furtherance of strategic partnerships, the aggressive engagement of relevant law enforcement, and the extensive use of liaison, operational support, and coordination.
The VCACITF (formerly known as the Innocent Images International Task Force) became operational on October 6, 2004 and serves as the largest task force of its kind in the world.

The VCACITF consists of online child sexual exploitation investigators from around the world and includes more than sixty-nine active members from forty countries. The task force hosts a five-week training session for newly invited task force officers, bringing them to the United States to work side-by-side with FBI agents in the Violent Crimes Against Children program. The VCACITF also conducts an annual case coordination meeting where task force members come together in a central location to share best practices and coordinate transnational investigations between members. Ireland, through the Garda Síochána is an active member of the VCACITF.

Ireland, through the Garda Síochána, engages proactively with Europol, Interpol and the law enforcement authorities in EU Member States and further afield, relating to a wide range of initiatives with an international dimension, which are designed to tackle child sexual exploitation.

The Garda Síochána will continue to develop its capacity to tackle cybercrime with a particular focus on protecting children and young people from the impact of the criminality involved and in this regard will interact in an appropriate manner with all relevant stakeholders.